18:3 BERKELEY TECHNOLOGY LAW JOURNAL

2003

Pages
773
to
944

Production: Produced by members of the *Berkeley Technology Law Journal* on PC computers. All editing and layout is done using Microsoft Word.

Printer: Joe Christensen, Inc., Lincoln, Nebraska.
Printed in the U.S.A.
The paper used in this publication meets the minimum requirements of American National Standard for Information Sciences—Permanence of Paper for Library Materials, ANSI Z39.48—1984.

Berkeley Technology Law Journal
University of California, Berkeley
Boalt Hall School of Law
587 Simon Hall
Berkeley, California 94720-7200
(510) 643-6454 (Phone)
(510) 643-6816 (Fax)
btlj@law.berkeley.edu
www.btlj.org

BERKELEY TECHNOLOGY LAW JOURNAL

VOLUME 18 NUMBER 3 SUMMER 2003

TABLE OF CONTENTS

ARTICLES

DONORS

The *Berkeley Technology Law Journal* acknowledges the following generous donors to Boalt Hall's Law and Technology Program:

Benefactors ($25,000 and above)

COOLEY GODWARD LLP
San Francisco, CA

FARELLA BRAUN + MARTEL LLP
San Francisco, CA

FENWICK & WEST LLP
Palo Alto, CA

GRAY CARY WARE & FREIDENRICH, LLP
Palo Alto, CA

HELLER EHRMAN WHITE & MCAULIFFE LLP
San Francisco, CA

LATHAM & WATKINS
San Francisco, CA

MILBANK, TWEED, HADLEY & MCCLOY LLP
Palo Alto, CA

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
Palo Alto, CA

WEIL, GOTSHAL & MANGES LLP
Redwood Shores, CA

WILSON SONSINI GOODRICH & ROSATI
Palo Alto, CA

Members ($10,000 to $24,999)

ALSCHULER GROSSMAN STEIN & KAHAN LLP
Los Angeles, CA

BINGHAM MCCUTCHEN
San Francisco, CA

COVINGTON & BURLING
San Francisco, CA

DAY CASEBEER MADRID & BATCHELDER LLP
Cupertino, CA

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
Palo Alto, CA

FISH & RICHARDSON P.C.
Redwood City, CA

GIBSON, DUNN & CRUTCHER LLP
Palo Alto, CA

KIRKLAND & ELLIS
San Francisco, CA

MAYER, BROWN, ROWE & MAW
Palo Alto, CA

MCDERMOTT, WILL & EMERY
Menlo Park, CA

MORRISON & FOERSTER LLP
San Francisco, CA

O'MELVENY & MYERS LLP
San Francisco, CA

ORRICK, HERRINGTON & SUTCLIFFE LLP
San Francisco, CA

PILLSBURY WINTHROP LLP
San Francisco, CA

SHEARMAN & STERLING
San Francisco, CA

TOWNSEND AND TOWNSEND AND CREW LLP
San Francisco, CA

Patrons ($5,000 to $9,999)

BAKER & MCKENZIE
Palo Alto, CA

DEWEY BALLANTINE LLP
Palo Alto, CA

FISH & NEAVE
Palo Alto, CA

HOWREY SIMON ARNOLD & WHITE LLP
Menlo Park, CA

IRELL & MANELLA LLP
Century City, CA

KEKER & VAN NEST LLP
San Francisco, CA

KENYON & KENYON
San Jose, CA

KNOBBE MARTENS OLSON & BEAR
Newport Beach, CA

MANATT, PHELPS & PHILLIPS LLP
Palo Alto, CA

MUNGER, TOLLES & OLSON
San Francisco, CA

VAN PELT & YI LLP
Cupertino, CA

Comment Competition Prize Sponsor

COOLEY GODWARD LLP
San Francisco, CA

The *Berkeley Technology Law Journal* is a nonprofit organization and welcomes donations. Donors are recognized appropriately for their contributions. For more information, contact the Development Editor, *Berkeley Technology Law Journal*, 587 Simon Hall, Boalt Hall School of Law, University of California, Berkeley, California 94720, (510) 643-6454, or e-mail btlj@law.berkeley.edu.

ADVISORY BOARD

SUBSCRIBER INFORMATION

The *Berkeley Technology Law Journal* (ISSN 1086-3818), a continuation of the *High Technology Law Journal* effective Volume 11, is edited and published four times each year (Spring, Summer, Fall, and Annual Review of Law and Technology) by the students of Boalt Hall School of Law, University of California, Berkeley.

Correspondence. Address all correspondence regarding subscriptions, address changes, claims for nonreceipt, single copies, advertising, and permission to reprint to Kira Abrams, Journal Publications Coordinator, 440 North Addition, Boalt Hall School of Law, Berkeley, California 94720-7200; (510) 643-6600; journalpublications@law.berkeley.edu. Authors: see section entitled Information for Authors.

Subscriptions. Annual subscriptions are $65.00 for individuals, and $85.00 for organizations. Single issues are $27.00. Please allow two months for receipt of the first issue. Payment may be made by check, international money order, or credit card (MasterCard/Visa). Domestic claims for nonreceipt of issues should be made within 90 days of the month of publication; overseas claims should be made within 180 days. Thereafter, the regular back issue rate ($27.00) will be charged for replacement. Overseas delivery is not guaranteed.

Form. The text and citations in the *Journal* conform generally to the UNITED STATES GOVERNMENT PRINTING OFFICE STYLE MANUAL (28th ed. 1984) and to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia Law Review Ass'n et al. eds., 17th ed. 2000). Please cite this issue of the *Berkeley Technology Law Journal* as 18 BERKELEY TECH. L.J. ___ (2003).

Postmaster: Send address changes to the *Berkeley Technology Law Journal*, University of California, Berkeley, Boalt Hall School of Law, 587 Simon Hall, Berkeley, California 94720-7200.

BTLJ ONLINE

Abstracts of all *Berkeley Technology Law Journal* and *High Technology Law Journal* articles as well as the full text of most articles published in previous issues can be found at http://www.btlj.org. Our site also contains subject, author and title indexes, general information about the *Journal*, selected materials related to technology law, and links to other related home pages. Subject, author and title indexes may also be found in Volume 10, Number 2 (1995) of the *Journal*.

INFORMATION FOR AUTHORS

The Editorial Board of the *Berkeley Technology Law Journal* invites the submission of unsolicited manuscripts. Submissions may include previously unpublished articles, essays, book reviews, case notes, or comments concerning any aspect of the relationship between technology and the law. If any portion of a manuscript has been previously published, the author should so indicate.

Format. Authors should submit double-spaced, single-sided manuscripts with generous margins. We regret that submissions cannot be returned. Authors should retain an exact copy of any material submitted. Authors may submit manuscripts in electronic or hardcopy form, though electronic submissions are strongly encouraged. Electronic submissions should be sent as attachments in Microsoft Word format to btlj@law.berkeley.edu.

Citations. All citations should conform to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia Law Review Ass'n et al. eds., 17th ed. 2000). In addition, the author should include his or her credentials, including full name, degrees earned, academic or professional affiliations, and citations to all previously published legal articles.

Copyrighted Material. If a manuscript contains any copyrighted table, chart, graph, illustration, photograph, or more than eight lines of text, the author must obtain written permission from the copyright holder for use of the material. A photocopy of such written permission should accompany the submission.

Mailing Address. Please submit all hardcopy manuscripts to:

Submissions Editor
Berkeley Technology Law Journal
University of California, Berkeley
Boalt Hall School of Law
587 Simon Hall
Berkeley, California 94720
(510) 643-6454 (Phone)

BOARD OF EDITORS 2003-2004

BALANCING PRIVATE RIGHTS AND PUBLIC POLICIES: RECONCEPTUALIZING PROPERTY IN DATABASES

By Jacqueline Lipton†

ABSTRACT

This Article presents a new paradigm for thinking about intangible property rights in response to recent criticism that information products such as databases should not be over-propertized. Analyzing the inherent problems with existing approaches, the Article concludes that creating private property rights in these intangible assets will not inevitably lead to commercial and social problems. On the contrary, legislatures can create private property rights that when accompanied by appropriate oversight and monitoring will preserve commercial markets and the public domain of information. Indeed, a new database law can use the concept of property as an organizing tool to properly balance private rights and the public policies. In developing this new approach to database protection, this Article examines the international debate on the creation of private property rights in databases. Furthermore, unlike previous models for *sui generis* database protection law based on copyright or trade secret law, the model in this Article draws on the principles underlying trademark and patent law in reaching a new solution.

---

† Assistant Professor, Case Western Reserve University School of Law; 11075 East Boulevard, Cleveland, Ohio 44106, USA; Email: JDL14@cwru.edu; Fax: + 1 216 368 2086; B.A. (Melb), B.A. (Hons) (La Trobe), LL.B (Hons) (Melb), LL.M (Monash), LL.M (Cambridge), Ph.D. (Griffith), Barrister and Solicitor of the Supreme Court of Victoria and the High Court of Australia. The author would like to thank Professor Andrew Morriss, Professor Peter Gerhart, Professor Craig Nard, Professor George Dent, Professor Michael Heise, Professor Cynthia Ho, Professor Sara Nelson, and Professor Mark Lemley for their comments on earlier drafts of this Article, as well as Mark Davison and Catherine Colston for useful information about database law in the European Union. The author would further like to thank participants in the Second Annual Intellectual Property Scholars' Conference at Cardozo Law School, New York City, August 8-9, 2002 for their helpful comments, as well as the participants in the ISLAT/IASTED Third Annual Law and Technology Conference, Boston, November 6-7, 2002. Finally, the author would like to thank Amy Noss for her valuable research assistance. All views expressed herein and any errors or omissions are those of the author.

TABLE OF CONTENTS

I. INTRODUCTION

In the general discussion over whether to recognize intellectual property rights in various areas of digital technology, the debate over proprietary rights in databases has raised many difficult questions. What should be the extent of the database rights? What are the ways in which these rights can be implemented? *Can* producers of databases claim these rights? *Should* they be able to claim these rights?

Databases span a wide range of fields. Some commercial and government databases contain consumer data—spending habits,[1] health, insurance, or financial status.[2] Other databases, some combining commercial and non-commercial uses, contain scientific, technological, or educational information.[3] Some commercially valuable databases may form the core of a company's business operations in areas such as travel planning,[4] stock brokeraging,[5] and online shopping.[6] Finally, some databases are relatively mundane compilations, such as phone books, but

---

1. Many major supermarket chains and other large department stores compile consumer spending information to enable targeted marketing. Allison Kidd, *A Penny Saved, A Lifestyle Learned? The California and Connecticut Approaches to Supermarket Privacy*, 4 N.C. J.L. & TECH. 143, 144-45 (2002).

2. Private financial institutions and insurance companies maintain their own customer records, while governments may collect health records and credit reporting agencies financial information on a widespread basis. Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN. L. REV. 85, 107 (2002); Rick S. Lear & Jefferson D. Reynolds, *Your Social Security Number or Your Life: Disclosure of Personal Identification Information by Military Personnel and the Compromise of Privacy and National Security*, 21 B.U. INT'L L.J. 1, 15 (2003).

3. These would include databases of profession-specific information such as LEXIS and Westlaw as well as more scientific and technical information. *See* Genomes OnLine Database, Integrated Genomics, Inc., *at* http://www.genomesonline.org/ (last visited July 24, 2003); Geographic Names Information System, U.S. Geo. Survey *at* http://geonames.usgs.gov/ (last visited July 22, 2003); NIST Scientific & Technical Databases, Nat'l Inst. of Standards & Tech., *at* http://www.nist.gov/srd/online.htm (last visited July 24, 2003).

4. Online travel agencies such as Expedia, Travelocity, and Orbitz maintain comprehensive databases of airline schedules and prices, hotel accommodations, car rental agencies, consumer trip planners, etc. *See, e.g.*, Expedia, *at* http://www. Expedia. com.

5. Financial institutions and financial planning companies keep large databases of stock prices.

6. An obvious example involves the comprehensive databases maintained by Amazon.com involving consumer preferences, books, and other products in stock, consumer reviews, etc.

may still have commercial value and raise questions about proprietary protection.[7]

Some of these databases should have associated proprietary and quasi-proprietary rights.[8] Realistically, property rights probably cannot be avoided if the market demands them. Establishing property rights by applying the concept of property to databases should not lead inevitably, as some critics suggest, to unfair information monopolies. Rather, legislatures can use property rights as a tool to strike an appropriate balance between private and public interests in database information.

The structure and content of database law should clearly evidence its purpose: to serve the needs of commerce by giving artificial lead time[9] to those who have invested time, effort, or financial resources in developing commercial databases. However, current debate ignores this purpose for the most part, focusing instead on the need for *sui generis* legislation protecting the contents of a database based on a copyright model. This misplaced focus on copyright models in the United States arises from perceived failings of copyright law to adequately protect databases in the wake of the Supreme Court's decision in *Feist Publications v. Rural Telephone Service Co.*[10] In *Feist*, the Supreme Court held that only databases showing some degree of originality in the selection, arrangement, or organization of their contents could merit copyright protection.[11] In reaching this holding, the Court rejected that the investment of time, effort, or money could justify protection. Because of *Feist's* holding, discussions about intellectual property rights in databases

---

7. Feist Publ'ns v. Rural Tel. Serv. Co., 499 U.S. 340 (1991) (holding that a white pages telephone directory was not protected under copyright law); *see also* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996) (upholding a shrinkwrap license prohibiting the copying of a digital telephone directory contained in commercial software).

8. There is no empirical evidence about the need for property rights in databases, but anecdotal evidence suggests that there may indeed be such a need in commerce. Justin Hughes, *Political Economies of Harmonization: Database Protection and Information Patents* 89-90 (Cardozo Law School, Public Law Research Paper No. 47, 2002), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=318486 (last visited Aug. 24, 2003) (discussing the political and market forces behind the debates for database protection legislation in the United States and in other jurisdictions).

9. I base this Article's proposition on the argument that database producers deserve some legally-created "lead time" to exploit their work to overcome market failures that may otherwise arise because of the ease with which competition can now copy and disseminate information compiled by the original database producer. J.H. Reichman & Pamela Samuelson, *Intellectual Property Rights in Data?*, 50 VAND. L. REV. 51, 145-58 (1997).

10. 449 U.S. at 359-60.

11. *Id.* at 348.

tend to begin with assumptions derived from copyright law and relating to copying conduct.

This focus on copyright principles is significantly flawed. When applied to commercial databases, models based on copyright principles encourage the creation of overbroad private rights in large volumes of information. The European Union, for example, currently overprotects databases.[12] Moreover, attempts to carve out fair use exceptions based on copyright law further complicate the application of copyright principles to digital databases.[13] Thus, the focus of the debate must move away from models that draw mainly on copyright law.

In the United States, laws based on a hybrid of copyright and trade secret law known as the "tort/misappropriation model" have been proposed.[14] The tort/misappropriation model still suffers from the legacy of copyright by creating a broad definition of a protected database followed by a list of vague fair use exceptions, but it may be preferable in some ways to pure copyright models.[15] The advantage of a tort/misappropriation model is that it focuses on "commerce" and "unfair conduct in commerce"—principles better suited to database protection than copyright's focus on protecting artistic and creative works[16] against

---

12. Catherine Colston, *Sui Generis Database Right: Ripe for Review?*, 3 J. INFO., L. & TECH. 4, §§ 2.2, 3.2 (2001), *at* http://elj.warwick.ac.uk/jilt/01-3/colston.html (last visited Aug. 24, 2003); Reichman & Samuelson, *supra* note 9, at 76-77.

13. Part of the difficulty is in clearly defining the scope of fair use exceptions to copyright infringement in the digital age. *See* 17 U.S.C. § 107 (2000); MARK LEMLEY ET AL., 3 SOFTWARE AND INTERNET LAW, 109-10 (2d ed. 2003) (describing the difficulties courts have had in interpreting the fair use factors in copyright cases). These problems should not be carried over into any new database laws.

14. *See* discussion *infra* Parts II-IV. On suggestions for developing a database law modeled on a tort/misappropriation model drawing from the law of trade secrets, see Reichman & Samuelson, *supra* note 9, at 80-81.

15. 17 U.S.C. § 107 (providing a fair use defense to copyright infringement where copying is undertaken for "purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research"). Consumer and Investor Access to Information Bill, H.R. 1858, 106th Cong. (1999). In determining whether a particular use is a fair use, courts take into account four factors:

> (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.

17 U.S.C. § 107.

16. 17 U.S.C. § 102 (describing the subject matter of copyright in terms of various listed "original works of authorship").

unauthorized reproduction.[17] Again, however, granting broad protections subject to fair use exceptions creates uncertainties and limits the utility of laws based on this model.

As explained in this Article, the better approach to database protection legislation is a model based on the underlying principles of trademark and patent registration.[18] This model uses a combination of market and government regulation to replace the strongly market-focused approaches inherent in both the copyright and tort/misappropriation models. Legislation based on this model would create a government authority to oversee a register of database rights, applications for registration, compulsory licensing, and the release of certain database contents into the public domain. Ultimately, a legislature could empower the administrative authority to resolve disputes among database creators, their competitors, and those who seek access to the contents of a database.

In contrast to this regulation model, many commentators have argued that the state should avoid regulating commercial databases as intellectual property principally because they view less state regulation as generally better.[19] For example, Professor Lawrence Lessig notes that in the twentieth century's global debate over whether the market or state is better suited to regulate the allocation and control of society's resources, the market has usually trumped the state.[20] These victories were based on the belief that markets worked better than the state in regulating resources[21] and that "whatever problems there are with the market, the problems with government are far more profound."[22] Professor Lessig suggests that

17. 17 U.S.C. § 501 prohibits violation of any of the exclusive rights of a copyright owner set out in the Copyright Act. These exclusive rights relate to reproduction and distribution, derivative works, and public performance. *See also* 17 U.S.C. § 106.

18. For example, this new model would limit protection to bona fide commercial uses of databases in identified markets and incorporate a registration system for relevant rights in databases.

19. *See, e.g.*, REGULATION WITHOUT THE STATE . . . THE DEBATE CONTINUES (John Blundell & Colin Robinson eds., 2000); Solveig Singleton, Self-Regulation: Regulatory Fad or Market Forces?, CATO WHITE PAPERS AND MISC. REPORTS, May 7, 1999 *at* http://www.cato.org/pubs/wtpapers/990507report.html; Ugnius Trumpa, *Does State Regulation Protect Consumers?*, THE FREE MARKET (Lithuanian Free Market Inst., Lithuania), Apr.-June 1998, *at* http://www.freema.org/NewsLetter/regulation/1998.2.state.phtml (last visited Aug. 27, 2003).

20. LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 12 (2001).

21. *Id.*

22. *Id.* (discussing theory of Ronald Coase).

certain resources should not be regulated at all, but should rather be left "free"[23] in the First Amendment sense of the term.[24]

However, are these underlying assumptions are correct? Should the market trump the state in all contexts? How can we presume that the government will always cause more profound problems than the market when creating and regulating rights in information resources when we have functioning state-run regimes in trademark and patent law?

Despite the anti-regulatory sentiment, governments in many areas of law have traditionally overseen and monitored statutory property rights.[25] Surprisingly, however, this governmental oversight has not spread to the regulation of intangible assets.[26] If a government is prepared to create new digital information property rights, such as existing laws in the European Union and proposed legislation in the United States,[27] it should also be prepared to take some control over the allocation and regulation of these property rights.

The information products market represents many important and competing interests. Because of the complex mixture of public and private interests in the information contained in databases, it is impertive that the government oversee the rights created in these databases. Market players seeking to commercially exploit databases obviously desire private property rights in databases. This desire for rights, however, must be balanced against competing public and private interests in database information. For example, individuals may have a privacy interest in personal information stored in certain databases like those compiling

---

23. *Id*.

24. *Id.* (Richard Stallman, who advocates that some information should be "free" in the sense of "free speech" rather than in the sense of "free beer").

25. *See* Bruce Yandle & Andrew P. Morriss, *The Technologies of Property Rights: Choice Among Alternative Solutions to Tragedies of the Commons*, 28 ECOLOGY L.Q. 123, 148 (2001) (arguing that statutory law creates a "strong incentive" for government involvement in a real property context).

26. Although some degree of government oversight is seen in traditional intellectual property law in the patent and trademark context, it has been lacking with respect to, say, property rights in copyright works in the digital age. Whereas patent and trademark applications are examined in detail prior to registration, copyright is very much asserted and commercially exploited at the right-holder's discretion. *See* discussion *infra* Part II.

27. Relevant legislative iniatives include: in the European Union, Council Directive 96/9/EC on the Legal Protection of Databases, 1996 O.J. (L 77) 20 [hereinafter E.U. Directive]; in the United States, the Collections of Information Antipiracy Bill of 1999, H.R. 354, 106th Cong. (1999), and the Consumer and Investor Access to Information Bill of 1999, H.R. 1858, 106th Cong. (1999).

consumer spending habits.[28] Consumers may have an interest in knowing information about products they purchase. Scientists, technologists, and educators have an interest in accessing database contents for non-commercial teaching and research.[29]

An important reason for advocating governmental rather than market force regulation of these property rights is that pure market control may not be able to properly regulate a market where the market players that are lobbying the legislatures to *create* statutory private property rights are the same players seeking to subsequently exploit the rights. If the government must create the relevant private property rights, a market in those rights might well be unable to regulate itself without some government assistance.[30]

Furthermore, markets in information products tend to be valuable and volatile.[31] They also often involve many competing interests that the market players are not interested in protecting.[32] Therefore, some government oversight may be needed to prevent unjustifiable information monopolies and to balance competing rights and interests in information for the good of commerce and society.

Finally, many information products, including some databases, are purely commercial. As seen recently with digital copyrighted works, market forces have a limited ability to deal with non-commercial aspects

---

28. Ann Bartow, *Our Data, Ourselves: Privacy, Propertization, and Gender*, 34 U.S.F. L. REV. 633, 633-34 (2000); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1284 (2000).

29. J.H. Reichman & Paul F. Uhlir, *Database Protection at the Crossroads: Recent Developments and Their Impact on Science and Technology*, 14 BERKELEY TECH. L.J. 793, 809-10 (1999).

30. *See* Yandle & Morriss, *supra* note 25, at 164-67.

31. *See* Bartow, *supra* note 28, at 647 (on the value of information markets in the digital age, particularly in the targeted marketing context); Litman, *supra* note 28, at 1290 (noting value of information markets and that some groups, notably consumers, often lose control over information in such markets); Pamela Samuelson et al., *A Manifesto Concerning the Legal Protection of Computer Programs*, 94 COLUM. L. REV. 2308, 2314, 2338 (1994) (characterizing software as an information product that is more vulnerable than traditional manufactured goods to market-destructive appropriations because of the applied industrial know-how born on or near the surface of software products).

32. For instance, how can we protect personal privacy rights and fair uses of information when private property interests invade the "information domain"? *See* 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, 360-64 (1999); Litman, *supra* note 28, at 1306-09.

of these products.[33] For example, the copyright industry successfully lobbied both for increased copyright protection terms[34] and amendments to the Copyright Act that support technological protection for digital copyright.[35] In these cases, market players have shown little interest in preserving the public domain or fair use rights.[36]

Regardless of whether particular governments take an interest in creating property rights in information, some form of property or quasi-property in information will undoubtedly develop if that information has commercial value and market players desire to exploit it.[37] As seen in digital information markets, market players have used contract and technological protection to control information for commercial exploitation despite the lack of statutory or judicially-created property rights in information.[38] Thus, we should not necessarily oppose the

---

33. *See* Benkler, *supra* note 32, at 411; Jacqueline Lipton, *Copyright in the Digital Age: A Comparative Survey*, 27 RUTGERS COMPUTER & TECH. L.J. 333, 358 (2001) [hereinafter Lipton, *Comparative Survey*]; David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 714 (2000); Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 BERKELEY TECH. L.J. 519, 537-46 (1999).

34. Sonny Bono Copyright Term Extension Act § 102, 17 U.S.C. § 302 (2000) [hereinafter CTEA]. A challenge to the validity of this legislation was argued and defeated before the Supreme Court in *Eldred v. Ashcroft*, 537 U.S. 186 (2003).

35. Digital Millennium Copyright Act (codified as amended in scattered sections of 18 U.S.C. (2000)) [hereinafter DMCA]. Note that these provisions may not prove effective against some hackers.

36. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 323-24 (S.D.N.Y. 2000), *aff'd*, 273 F. 3d 429 (2d Cir. 2001) (holding that the fair use provisions of the Copyright Act cannot be used as a defense to an infringement of the DMCA's anti-circumvention and anti-trafficking provisions as this was not the legislative intent of 17 U.S.C. § 1201(a)); Benkler, *supra* note 32, at 356-57; Nimmer, *supra* note 33, at 702-10; Samuelson, *supra* note 33, at 537-46; John R. Therien, *Exorcising the Specter of a "Pay-Per-Use" Society: Toward Preserving Fair Use and the Public Domain in the Digital Age*, 16 BERKELEY TECH. L.J. 979, 1008-10 (2001) (writing about concerns that the DMCA will over-propertize digital information if courts do not take an adequate stance on protecting fair uses).

37. RAYMOND NIMMER, 1 THE LAW OF COMPUTER TECHNOLOGY, ¶ 3.02[1] (3d ed. 1997) (noting that trade secrets are described as "property" by American courts and legislators, despite the fact that they do not evidence significant elements from traditional property theory, precisely because of the need for markets effectively to transact with the relevant information); Litman, *supra* note 28, at 1290-93 (making similar observations in the information property context).

38. ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1455 (7th Cir. 1996) (upholding shrinkwrap license in a "pure" information product in the form of a digital telephone directory); William W. Fisher III, *Property and Contract on the Internet*, 73 CHI.-KENT L. REV. 1203, 1249 (1998) (observing how contract and technological measures are taking over from reliance on statutory property rights in protecting information products

creation of property rights in information by courts and legislatures so long as these institutions are vigilant about *limiting* the rights in ways that support the realistic commercial needs of rights-holders without encroaching unnecessarily into the public domain of information and ideas, or the competing private interests in relevant information, such as personal privacy rights.

Many of the arguments made in the following discussion of property rights in databases may become broadly applicable to other parts of intellectual property law, notably to U.S. copyright law in the wake of the enactment of the Digital Millennium Copyright Act ("DMCA").[39] By focusing here on the potential of collections of information to comprise information property rights, the kinds of limitations or regulations that may operate in this context, and the appropriate amount and nature of government oversight, this Article may provide a useful guide for thinking about the law relating to future digital property rights.

Part II considers the nature of a compilation of information, or "database," and attempts to identify and significantly restrict the types of databases likely to warrant protection under any new private property regime in the United States. The criteria for legislative protection arise from the realistic commercial objectives of rationally self-interested database producers.[40] Any new database protection law should be clearly addressed to these objectives, and should not operate any more broadly than necessary to achieve these ends. Furthermore, Part II argues that in defining the appropriate scope of the private property rights with respect to the commercial objectives of database producers, Congress should not make the mistake of concluding that the market alone should regulate the commercial exploitation of those rights. The government should be ready to take on a significant monitoring and controlling role, particularly where property rights in information per se are implicated.[41]

---

from unauthorized interference, and in transacting with information); Michael J. Madison, *Legal-Ware: Contract and Copyright in the Digital Age*, 67 FORDHAM L. REV. 1025, 1054-76 (1998) (observing how contractual licenses are overtaking proprietary copyrights as the mechanism for commercial exploitation of valuable digital information products).

39. *See* DMCA, *supra* note 35; Benkler, *supra* note 32, at 414-15; Lipton, *Comparative Survey*, *supra* note 33, at 339-44; Nimmer, *supra* note 33, at 674-75; Samuelson, *supra* note 33, at 558.

40. *See* Mary Maureen Brown, Robert M. Bryan, & John M. Conley, *Database Protection in a Digital World*, 6 RICH. J.L. & TECH. 2, ¶ 35 (1999), *at* http://law.richmond.edu/jolt/v6i1/conley.html.

41. *See* Litman, *supra* note 28, at 1294-95 (describing the downsides of creating private property rights in information).

Part III turns to some of the major shortcomings of existing laws in protecting private property rights in databases, notably copyright law and trade secret law. It also critically examines models for new *sui generis* database protection legislation in the United States and European Union.

Part IV suggests new approaches to *sui generis* laws that deal with the creation and commercial exploitation of property rights in databases. The new approaches draw significantly from those aspects of trademark and patent law that require some government oversight of private property rights in commercially valuable information products.

Part V considers some of these suggestions within a broader international context because of the increasingly global nature of information commerce. There is some concern that U.S. legislation could end up clashing with the European Union's Directive on the Legal Protection of Databases ("E.U. Directive"),[42] which is already in place throughout the European Union and which could disadvantage American businesses abroad.[43] The E.U. Directive has been criticized for creating too much protection for databases and too little protection for public interests in their contents.[44] The United States currently has a chance to lead the way in effective and efficient database protection legislation at the international level; however, Congress must act quickly, before the E.U. position becomes entrenched as the global standard.

Finally, Part VI presents some conclusions about the need for a database protection model that can effectively balance private rights and public interests in database contents, and the present opportunity for the United States to take a leadership role in harmonizing this increasingly important aspect of intellectual property law across international lines.

---

42. E.U. Directive, *supra* note 27.

43. As will be apparent from the following discussion, many would argue that the E.U. approach to database protection legislation has been a failure, or at least a highly questionable legislative measure, partly because of the lack of clear delineation of the rights in question by the government and arguably also because of the lack of ongoing government oversight in relation to the commercial exploitation of those rights.

44. Colston, *supra* note 12, §§ 3.2-3.3. Unfortunately, a number of models for American database protection legislation to date evidence similar problems. Reichman & Samuelson, *supra* note 9, at 77.

II. COMPILATIONS OF INFORMATION

A. The Nature of Information Compilations and the Regulatory Impulse

1. The Vulnerability of Compiled Information

In an age in which information is more readily available and more valuable than ever before, products made up of pure information are also more vulnerable in commerce.[45]

Some information products such as customer lists, spending profiles of particular people, or the television viewing preferences of particular groups may contain personal information.[46] Other products such as business directories, event calendars, timetables, product catalogues, or supplier and distributor lists may contain more impersonal information. These products have always had undeniable commercial value, particularly for marketing and tailoring new products and services to better match consumer needs.[47] Today, an unprecedented amount of information can be collected, collated, and re-presented in accessible, flexible ways in order to meet particular user needs. For example, a user may search airline databases for flights based on a specified itinerary, price range, and time; and then arrange the results according to the user's priorities.[48] However, as user flexibility expands, the ease with which information can be accessed electronically and perfectly copied by commercial competitors is also increasing.[49] This presents a challenge for intellectual property law.

Traditional intellectual property is poorly suited to protecting database products.[50] Patent law will not work: an information product's value is in the information per se, not in any patentable invention. Under copyright law, the selection or arrangement of a database's contents is often not

---

45. COMM. TO STUDY GLOBAL NETWORKS & LOCAL VALUES, NAT'L RESEARCH COUNCIL, GLOBAL NETWORKS AND LOCAL VALUES: A COMPARATIVE LOOK AT GERMANY AND THE UNITED STATES 176 (2001); Rex Y. Fujichaku, *The Misappropriation Doctrine in Cyberspace: Protecting the Commercial Value of "Hot News" Information*, 20 U. HAW. L. REV. 421, 428 (1998); Samuelson et al., *supra* note 31, at 2337-38.

46. *See* Litman, *supra* note 28, at 1283-84.

47. *See* Bartow, *supra* note 28, at 643-50.

48. Jonathan A. Weininger, *Trademark Metatagging: Lanham Act Liability or Pareto Optimality?* 23 WHITTIER L. REV. 469, 473 (2001) (explaining use of search engines on the Internet in terms of accommodating specific user requests).

49. MARGARET RADIN ET AL., INTERNET COMMERCE: THE EMERGING LEGAL FRAMEWORK 629-30 (2002).

50. *Id.*

sufficiently original to warrant protection.[51] In fact, the value of a commercial online database often lies in the very comprehensiveness and non-selectivity of its contents.[52]

Furthermore, trade secret law will only protect a commercial database if everyone who has access to the database, both authorized and unauthorized, has agreed to a confidentiality agreement enforceable in both national and foreign courts.[53] This involves high transaction costs, making this form of protection impracticable. Thus, patent, copyright, and trade secret law cannot effectively protect a producer's interest in a commercial database.

True, technological protection measures can serve as an interim measure to minimize unauthorized access to compilations of information.[54] However, such measures must constantly be updated or risk computer hackers cracking the technology and accessing or disseminating the protected information.[55] Laws, such as the anti-circumvention and anti-device provisions of the DMCA, can prohibit unauthorized cracking of encryption codes.[56] But legal enforcement may, in many cases, be the equivalent of shutting the barn door after the horse has bolted.[57] By the

---

51. *See* Feist Publ'ns v. Rural Tel. Serv. Co., 499 U.S. 340, 340 (1991) (rejecting the "sweat of the brow" doctrine).

52. Wesley L. Austin, *A Thoughtful and Practical Analysis of Database Protection Under Copyright Law, and a Critique of Sui Generis Protection*, 3 J. TECH. L. & POL'Y 3, 58 (1997), *available at* http://journal.law.ufl.edu/~techlaw/3-1/austin.html (last visited Aug 30, 2003); Brown, Bryan, & Conley, *supra* note 40, ¶ 46.

53. *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475 (1974) ("The protection accorded the trade secret holder is against the disclosure or unauthorized use of the trade secret by those to whom the secret has been confided under the express or implied restriction of nondisclosure or nonuse.")

54. Jacqueline Lipton, *Protecting Valuable Commercial Information in the Digital Age: Law, Policy and Practice*, 6 J. TECH. L. & POL'Y 2, 26-28 (2001), *available at* http://grove.ufl.edu/~techlaw/vol6/Lipton.htm (last visited Aug. 24, 2003) [hereinafter Lipton, *Commercial Information*].

55. NAT'L RESEARCH COUNCIL, A QUESTION OF BALANCE: PRIVATE RIGHTS AND THE PUBLIC INTERESTS IN SCIENTIFIC AND TECHNICAL DATABASES, ch. 3 (1999), *available at* http://www.nap.edu/html/question_balance/ch3.html (last visited Aug. 24, 2003).

56. DMCA, *supra* note 35, 17 U.S.C. §§ 1201(a)(1)(A), 1201(a)(2), 1201(b)(1) (2000).

57. For example, monetary compensation may be inadequate if damages are difficult to quantify or if the defendant is an impecunious computer hacker. Injunctions may also prove pointless to stop the dissemination of a decryption technology once the code is in the public domain. The spread of hacking code on the Internet can be rapid and global, and it may prove impossible for a court to grant an injunction that has any hope of stopping people the world over from using the decryption measure to access the relevant

time a court hears a case, the damage has already been done and whatever remedy the court may order would be inadequate to repair the damage.[58]

2. Enhanced Legal Protection For Compiled Information

Current discussion among lawmakers and members of the legal community shows a need for legislation to protect information compilations.[59] Given the value and vulnerability of information compilations, the next steps are to clearly identify the kinds of compilations that might merit some form of enhanced legal protection and then to determine what shape such protection should take. This is a timely and difficult issue that goes to the heart of the tensions in existing intellectual property law, both within the United States and internationally.[60] The debate will be most fruitful if conducted with this broader context in mind.

Notably, there is no empirical evidence available about actual or potential market failures in this area. Thus, some argue for foregoing any new legislation at all. This would allow the market to sort out the relevant issues using contractual provisions[61] and technological protection

---

work(s). A federal district court made this point in *Reimerdes*. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 344 (S.D.N.Y. 2000). The judge granted an injunction prohibiting the defendants from maintaining links on their websites to software that decrypted technical protection measures designed to prevent DVD copying, as well as links to other websites that maintained this software. *Id.* at 343. The judge was prepared to grant the injunction as a matter of principle, but noted that it may not be of much practical comfort to the plaintiff movie studios for the above reasons. *Id.* at 344-45. The decision was recently upheld on appeal. *See* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001), *available at* http://www.nyls.edu/samuels/copyright/beyond/cases/reimerdesapp6.htm (last visited June 18, 2002).

58. *Reimerdes*, 111 F. Supp. 2d at 344.

59. Telstra Corp. v. Desktop Mktg. Sys. Pty Ltd. (2001) F.C.A. 612, ¶ 83, *aff'd*, (2002) F.C.A.F.C. 112 (Austl.) (making Australian law the opposite of American law under *Feist* with respect to copyright in non-original databases, which may evidence the need to rethink database protection on a more global scale to achieve some measure of international harmonization), *available at* http://www.austlii.edu.au/au/cases/cth/federal_ct/2001/612.html (last visited Aug. 24, 2003); Brown, Bryan, & Conley, *supra* note 40, ¶¶ 61-64 ; Reichman & Samuelson, *supra* note 9, at 55.

60. DAVID LANGE ET AL., INTELLECTUAL PROPERTY: CASES AND MATERIALS, CH. 1 (1998); Reichman & Samuelson, *supra* note 9, at 52-53 (discussing the traditional distinction between what is protected by which particular form of intellectual property).

61. RONALD MANN & JANE WINN, ELECTRONIC COMMERCE 184-93 (2002); Margaret Radin, Online Standardization and the Integration of Text and Machine, 70 FORDHAM L. REV. 1125 (2002), *reprinted in* RADIN ET AL., *supra* note 49, at 362-65.

measures[62] while avoiding the potential danger of database protection legislation—a detrimental effect on the public domain of information.

However, leaving information protection of online databases to the market also involves certain risks. Laws now support "clickwrap" and "shrinkwrap" licenses of electronic information products.[63] They also support the widespread use of digital rights management: technical encryption measures that prevent access to certain electronically stored information.[64] Strengthened by these laws, market players that tend to have their own commercial interests at heart are unlikely to spend time and resources to implement systems to protect competing interests.

Designing a new database model that uses property rights to *limit* a database producer's ability to create market monopolies may be the most effective way to prevent database makers from using contractual and technological measures to create property rights that are impervious to any competing uses of the information.[65]

In today's global trading environment,[66] there is little point in enacting piecemeal new legislative measures that differ significantly between jurisdictions. Moreover, any such legislative initiatives must not destroy the current policies underlying patent, copyright, and trade secret law both within and among jurisdictions. For intellectual property law to remain a cohesive and useful system, each new legislative development must further the overriding aims and objectives of the law.[67]

---

62. RADIN ET AL., *supra* note 49, ch. 11 (providing an overview of technological protection measures).

63. *See, e.g.*, UNIF. COMPUTER INFO. TRANSACTIONS ACT § 209 (2001) [hereinafter UCITA]. UCITA has so far met with limited success in being adopted by state legislatures); *see also* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1447 (7th Cir. 1996); MANN & WINN, *supra* note 61, at ch. 4; RADIN ET AL., *supra* note 49, at 299-342; Madison, *supra* note 38, at 1049-54.

64. *See, e.g.*, DMCA, *supra* note 35, 17 U.S.C. §§ 201(a)(1)(A), 1201(a)(2), 1201(b)(1).

65. Julie Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 608-09 (2003) (describing ways in which public policies have trumped contractual restrictions in the past, and noting that the same could occur in relation to digital rights management technologies coupled with tight contractual restrictions on information access; that is, the government could impose legislation that overrides the use of technologies and contracts that restrict access to information in certain circumstances).

66. Matters of international harmonization in this area are taken up in more detail in the final part of this Article.

67. Jeffrey C. Wolken, *Just the Facts, Ma'am. A Case for Uniform Federal Regulation of Information Databases in the New Information Age*, 48 SYRACUSE L. REV. 1263, 1294-98 (1998).

However, it is equally important that new legislative initiatives actually be new. To date, the debate over intellectual property protection for databases has suffered from being too heavily focused on copyright models of database protection. New initiatives in database protection law must transcend the constraints of the copyright models and focus instead on identifying and addressing the realistic needs of commerce and public policy on compiled information.

In this context, moves toward new legislation must tackle, with specific reference to the types of information, the complex practical and theoretical questions surrounding the creation of new property or quasi-property rights. Important issues, for example, arise about using law to commodify compilations of information that is personal or that has significant educational, scientific, or technical applications. Furthermore, moves toward creating new law must be sensitive to concerns about freedom of information, privacy,[68] the needs of scientific and educational communities,[69] and the cultural differences that can underlie attitudes toward these issues in different jurisdictions.[70]

Furthermore, new legislative initiatives must discard the misplaced focus on the tension between property and tort/misappropriation models that has characterized the debate so far. Those that favor the latter model tend to do so because it does not expressly advocate property rights in information.[71] However, this distinction between the two models is flawed: both models involve property to some degree because something, property or quasi-property, must be the subject of the misappropriation.

3. Refocusing the Debate on Database Protection

Assuming a need for legislative action, we must confront the problem that recent approaches to database protection legislation, in both the European Union and the United States, have been born out of perceived failings of copyright law to adequately protect rights in commercially valuable databases and compilations. Thus, these approaches have

---

68. *See* Bartow, *supra* note 28, at 634; Lipton, *Comparative Survey*, *supra* note 33, at 364-65.

69. *See* PAUL A. DAVID, A TRAGEDY OF THE PUBLIC KNOWLEDGE 'COMMONS'? GLOBAL SCIENCE, INTELLECTUAL PROPERTY AND THE DIGITAL TECHNOLOGY BOOMERANG 4-7 (Oxford IP Research Centre, Working Paper No. 04/00, 2000), *available at* http://www.oiprc.ox.ac.uk/EJWP0400.html (last visited Aug. 24, 2003).

70. For example, the European Union has stronger privacy rights than the United States. *See* MANN & WINN, *supra* note 61, at 184-93.

71. Other differences between the two models include the duration of rights granted in information products, and the basis for calculation of damages for wrongful duplication or dissemination of protected information.

unproductively focused on modifying existing copyright models to suit database protection.[72]

It would be more useful to refocus the discussion on the types of databases that require legal protection and how best to achieve such protection, being mindful of the need to balance any newly created rights in databases against competing public and private interests in information.

First-generation proposals for database legislation should demonstrate restraint since it is generally easier to expand the reach of a law that initially achieves too little protection than it is to restrict the operation of a law that initially creates too much.[73] The right balance may come from thinking about using intangible property law to promote *commerce* rather than the expression of ideas. This would require shifting to models of intellectual property law historically developed to serve the needs of commerce, such as registered trademarks and trade secrets, away from those that originally served more artistic/expressive purposes, such as the law of copyright.[74] This is not to suggest that markets should necessarily be the sole source of *regulation* of such rights, rather that laws creating such rights should focus on supporting information commerce as a primary objective.

Anglo-American copyright law has a significant commercial focus when compared with traditional European models of copyright law.[75]

---

72. The E.U. Directive, for example, takes the copyright approach of creating a relatively broad intellectual property right that will endure for a fixed term of years, then carving fair use type exceptions out of the right. E.U. Directive, *supra* note 27, at 20. Some Bills introduced into the U.S. Congress have also taken this approach. An example is the Collections of Information Antipiracy Act, H.R. 354, 106th Cong. (1999), which will be discussed in more detail *infra*. Even those approaches that do not expressly create a broad proprietary right tempered with fair use exceptions, do envisage at least an implied property right, again subject to fair use exceptions. *See, e.g.*, Consumer and Investor Access to Information Act, H.R. 1858, 106th Cong. (1999). This will also be discussed *infra*. All these models assume that the market will largely regulate itself once the relevant rights and statutory prohibitions have been enacted.

73. Wolken, *supra* note 67, at 1297-98.

74. The original purpose of copyright was to protect artists and artistic, literary, dramatic, and musical works, rather than to protect commerce. DEBORAH BOUCHOUX, INTELLECTUAL PROPERTY: THE LAW OF TRADEMARKS, COPYRIGHTS, PATENTS, AND TRADE SECRETS 133-38 (2000). Copyright has clearly been used to enhance commerce, particularly in recent years. However, the underlying model of the law is perhaps less commercially focused than, say, trademark law. Even the definition of a trademark draws heavily on commercial concepts and "trademark" is defined in relation to its use in commerce. *See* 15 U.S.C. § 1127 (2000).

75. *See* Gilliam v. ABC, 538 F.2d 14, 24 (2d Cir. 1976); U.S. PAT. & TRADEMARK OFF., REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS: INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE 133-34

However, Anglo-American copyright law still protects "works of authorship"[76] as opposed to the purely commercial subject matter of trademark law and trade secret law. As the subject matter of a new law, commercial databases seem to be more analogous to trademarks and trade secrets than they are to copyrights.

Using copyright structures as the basis for new models of database protection law introduces several problems. First, creating broad property rights with vague fair use exceptions is not suited to the needs of commercial database producers or to those claiming access rights in database contents.[77] Furthermore, besides the simple registration process not even required to claim copyright protection,[78] copyright law calls for little government oversight of the copyright's commercial exploitation or of exploitation that might adversely affected particularly vulnerable classes of copyright users.[79]

This might be an appropriate approach for copyright regulation in the digital age, but it is clearly not the right approach for regulating non-original, non-creative compilations of information. Although a database producer may be entitled to some proprietary rewards for the expenditure of time, effort, or resources in compiling a commercially valuable database, the nature of the resulting asset calls for a private property regime that includes significant limitations on associated property rights, and some government oversight of the creation and exploitation of those rights.

B. Defining the Scope of Database Protection

1. Existing Definitions

One of the first problems in developing appropriate *sui generis* database protection law is to suitably define a "compilation of information" or "database." The definition should be limited to serving the

---

(Sept. 1995), *available at* http://www.uspto.gov/web/offices/com/doc/ipnii/lawcopy.pdf (last visited Aug. 7, 2003).

76. 17 U.S.C. § 102(a) (2000).

77. In fact, this traditional copyright scheme is increasingly unsuited to copyright holders and those seeking access to copyright works in the digital age. *See* Raymond Shih Ray Ku, *The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology*, 69 U. CHI. L. REV. 263, 322-24 (2002).

78. The United States is in the minority of countries that actually have a copyright register. COPYRIGHT OFFICES WORLDWIDE, United Kingdom Intellectual Property Website, http://www.intellectual-property.gov.uk/std/resources/copyright/offices_worldwide.htm (last visited Aug. 15, 2003).

79. *See* Benkler, *supra* note 32, at 427; Nimmer, *supra* note 33, at 693-99; Samuelson, *supra* note 33, at 537-546.

legislation's aims: balancing the commercial needs of database producers with public policy concerns about over-commodifying information. Existing models of database protection law have tended to include a definition of database much broader than required and largely derived from similar definitions in copyright law.[80] Adopting a more restricted definition of database can simplify new legislation by automatically limiting the rights derived from the defined item to relevant commercial activities. Moreover, such an approach minimizes the need to engage in a protracted debate about fair uses or permitted activities that we might otherwise wish to except as a matter of public policy from the activities prohibited under the legislation. If the definitions and associated rights are more tightly focused initially to protect limited commercial activities involving databases, then there is less need to create detailed fair use provisions, which tend to be problematic in both practice and theory.[81]

Existing laws that attempt to define the term "database" include the E.U. Directive and, in the United States, the Collections of Information Antipiracy Bill of 1999 ("Antipiracy Bill")[82] and the Consumer and Investor Access to Information Bill of 1999 ("Consumer and Investor Access Bill").[83] A look at these definitions suggests some directions for a more tailored approach.[84]

The E.U. Directive currently defines a database as "a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other

---

80. "Compilation" (rather than "database") is defined in the U.S. copyright legislation broadly as "a work formed by the collection and assembling of preexisting materials or of data that are selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship." The term "compilation" includes "collective works." 17 U.S.C. § 101. In the United Kingdom, the definition of "database" in the copyright legislation is arguably even broader. It encompasses "a collection of independent works, data, or other materials which (a) are arranged in a systematic or methodical way and (b) are individually accessible by electronic or other means." Copyright, Designs, and Patents Act, 1977, § 3A(1) (Eng.) [hereinafter CDPA].

81. *See* MARSHALL LEAFFER, UNDERSTANDING COPYRIGHT LAW 428 (3d ed. 1999); DAVID, *supra* note 69, at 5-6.

82. H.R. 354, 106th Cong. (1999).

83. H.R. 1858, 106th Cong. (1999).

84. Terms such as "database," "compilation," and "collection of information" have been defined variously, both colloquially and in legislation, throughout the world. For ease of reference, this discussion uses the term "database" in a generic sense to refer to all compilations or collections of information about which Congress may consider legislating.

means."[85] This definition tracks the wording of a proposed World Intellectual Property Organization ("WIPO") treaty on database protection that never entered into force.[86]

Definitions of database or equivalent terms in proposed U.S. legislation have been a little more detailed. For example, the Consumer and Investor Access Bill defines "database" as:

> [A] collection of discrete items of information that have been collected and organized in a single place, or in such a way as to be accessible through a single source, through the investment of substantial monetary or other resources, for the purpose of providing access to those discrete items of information by users of the database. However, a discrete section of a database that contains multiple discrete items of information may also be treated as a database.[87]

The reference here to a substantial investment of monetary or other resources derives from the idea that a *sui generis* database right should protect those databases in which producers make a substantial investment but which do not meet the standards of originality or creativity required by copyright law.[88] Absence of the investment criterion in the E.U. Directive's definition of database does not mean that it is irrelevant to E.U. law. Rather, the Directive addresses the issue in Article 7(1), where it creates a *sui generis* database right. Likewise, Rule 13(1) of the Copyright and Rights in Databases Regulations 1977 (Eng.) establishes an investment criterion.

Thus, overall the Consumer and Investor Access Bill takes a similar approach to the E.U. Directive in how it defines a database. However, the U.S. bill uses "items of information" to describe the likely contents of a database whereas the E.U. Directive refers to "works, data or other materials." This appears to mean that the European Parliament and Council of Ministers had a broader array of items in mind than the drafters of the Consumer and Investor Access Bill, as the latter law would only cover a collection of discrete *items* of information, such as a list of customers, as opposed to an electronic library of, say, copyright *works*,

---

85. E.U. Directive, *supra* note 27, art. 1(2).

86. World Intellectual Property Organization [hereinafter WIPO], Draft Treaty on Intellectual Property in Respect of Databases 2(i) (1996) (on file with the author), *available at* http://www.wipo.org/eng/diplconf/6dc_sta.htm (last visited Sept. 26, 2001) [hereinafter WIPO, Draft Treaty].

87. H.R. 1858 § 101(1).

88. See discussion of *Feist* case *supra* Part II.A.

such as books or journal articles (for example, LEXIS or Westlaw). This argument is bolstered by the definition of "information" in section 101(3) of the bill: "[F]acts, data, or any other intangible material capable of being collected and organized in a systematic way, *with the exception of works of authorship*."[89]

The idea behind this language is presumably that compilations of works of authorship are covered by section 103 of the Copyright Act and need not receive double protection as a result of any new database protection legislation enacted in the United States.[90] However, this argument is not particularly convincing, as compilations of facts or data are also protected by section 103. This suggests that the drafters of the copyright legislation saw no need to distinguish between the two types of compilations. On the other hand, both the customer list *and* the electronic library would meet the definition of database under European Union law, as the definition of the term in the E.U. Directive includes collections of "works" and "other materials" as well as "items of information."

Turning, then, to the definitions of "collection of information" and "information" found in section 2 of the Antipiracy Bill, which, if adopted, would add a new section 1401 to Title 17 of the United States Code ("U.S.C.") on copyright. Sequential drafts of this bill have put forth several versions of the definition of "collection of information,"[91] the most recent of which is:

> [I]nformation that has been collected and has been organized for the purpose of bringing discrete items of information together in one place or through one source so that persons may access them. The term does not include an individual work which, taken as a whole, is a work of narrative literary prose, but may include a collection of such works.[92]

---

89. H.R. 1858 § 101(3) (emphasis added).

90. *See supra* note 80. A "collective work" is defined as, "a work, such as a periodical issue, anthology, or encyclopedia, in which a number of contributions, constituting separate and independent works in themselves, are assembled into a collective whole." 17 U.S.C. § 101 (2000).

91. This Bill evidences a preference of the drafters for the "collection of information" terminology over the database terminology used in the E.U. Directive.

92. H.R. 354, 106th Cong., § 1401(1) (1999). This version of the Bill, dated October 8, 1999, is an amended version of the original Bill introduced into the House on January 19, 1999. The main difference in the definition of "collection of information" between the two versions is the inclusion of the second sentence of the definition in the amended version of the Bill, presumably to clarify that the legislation would not override the operation of existing copyright law in relation to narrative literary works.

This language clearly contemplates that both compilations of information/facts and compilations of works will qualify for protection under the new law. Yet an individual work will not, instead attracting copyright protection as a "literary work."[93]

The Antipiracy Bill also defines "information" as "facts, data, works of authorship, or any other intangible material capable of being collected and organized in a systematic way."[94] Note the similarity between this approach to the idea of "information" or "data" and that comprised in the E.U. Directive. Here, again, a broad brush definition indicates that a database might comprise electronic libraries of literary works as well as more basic lists of information.

Although these different legislative models vary somewhat in their approaches to defining a database or compilation of information, they all arguably craft their definitions much broader than necessary. If these laws were designed to create limited database rights that encourage commercial innovation and exploitation, why do the initial definitions fail to distinguish between different types of databases? The definitions in any new legislation should identify and cover only those databases created for exploitation in identifiable commercial markets.

2. Paper-Based Databases

The recent, rapid growth of e-commerce and other online activity has revolutionized the role of databases in business and other endeavors. Prior to the development of many commercially-valuable electronic databases, such as digital libraries,[95] there was little pressure on legislatures to enact *sui generis* database protection legislation. Since practical problems of database protection generally arise in the digital sphere, perhaps new legislative initiatives dealing with database protection should exclude the paper-based world and focus exclusively on digital databases. It is potentially much easier in practice to prevent unauthorized access to a physical library than to its digital counterpart.

Some commentators presume against paper by taking the view that database in today's market naturally refers to electronic, rather than physical, compilations of information. Carstens, for example, defines the term as follows:

---

93. 17 U.S.C. § 102(a)(1); *see also id.* § 101 (defining "literary work" as one that incorporates a work of narrative prose as a work "expressed in words, numbers, or other verbal or numerical symbols or other indicia, regardless of the nature of the material objects").

94. H.R. 354 § 1401(2).

95. Such as Westlaw, LEXIS, and SSRN.

> A data base [sic] is simply a set of data stored and accessed *by electronic means*. No limit is put on the amount of data involved or on its arrangement. It may be a collection of full-text materials or a compilation of extracts of works. It may be a collection of material in the public domain, such as lists of names and addresses, prices, or reference numbers. Lastly, it may consist of the *electronic publishing* of a single but voluminous work, such as the encyclopaedia. The common thread is that a data base requires effort to compile and arrange. A *computer program* aids the compilation and retrieval process by allowing the user to create or manipulate the data base in a variety of ways.[96]

The original version of the E.U. Directive limited the scope of the Directive to collections of work stored and accessed by electronic means.[97] However, some lawmakers argued that it would be difficult to limit legislation in such a way and that there may be no pragmatic reason for doing so.[98] Why should paper-based databases and compilations not attract the same protections as electronic versions, particularly where there has been a substantial investment of time, money or effort in their creation?[99]

There are some important differences between the nature and value of electronic and paper-based databases. An electronic database may be more comprehensive than a paper-based version, easier to update frequently, and more able to offer targeted searches tailored to the needs of individual users.

Those favoring legal protection for paper-based databases would argue that despite these differences both electronic and paper-based databases may involve a substantial investment of time, money, and effort. The value of both types lie in the contents of the database and the ease with which they can be searched. Both types may have commercial value. Furthermore, advances in scanning and optical character recognition technologies render even paper-based databases vulnerable to cheap and efficient copying in both hard copy and electronic form.[100]

---

96. David W. Carstens, *Legal Protection of Computer Software: Patents, Copyrights, and Trade Secrets*, 20 J. CONTEMP. L. 13, 16 (1994) (emphases added).

97. IAN LLOYD, LEGAL ASPECTS OF THE INFORMATION SOCIETY 178 (2000).

98. *Id.*

99. *Id.*

100. U.S. COPYRIGHT OFF., REPORT ON LEGAL PROTECTION FOR DATABASES 41 (August 1997), *available at* http://www.copyright.gov/reports/dbase.html (last visited Aug. 3, 2003). This may or may not be a realistic concern, as it is still arguably more difficult and time consuming to optically scan and copy a large paper-based database than

Nevertheless, most of the current problems in database protection involve electronic databases, which may or may not be electronic versions of databases that were originally paper-based.[101] The leading Supreme Court authority limiting copyright protection in databases, *Feist*,[102] involved a familiar form of paper-based database: a white pages telephone book. In *Feist*, the Court held that in order to qualify for copyright, a database must evidence some degree of originality in the selection or arrangement of its contents.[103] The white pages telephone book failed to satisfy this threshold test.

However, although this case was decided in 1991, database protection did not become a significant issue in the United States until recently when major electronic database producers began developing significant business interests in the United States and elsewhere.[104] This delay in addressing database protection may have occured because in the predominantly paper-based world of databases and compilations of over a decade ago it was easier to find enough creativity in the selection or arrangement of contents to establish copyright protection. The static, preformatted contents of paper-based databases tend to bear a unique imprimatur.

By contrast, in the electronic world, comprehensiveness, mutability, and functionality may add great commercial value to many large databases.[105] This distinction may provide good reason for limiting the definition of database in any new laws to electronic compilations, as such compilations often indicate the line where copyright usually ceases to apply.

Though the Court in *Feist* noted that "the vast majority of compilations" would pass its test for copyrightability,[106] the judges were

---

it is to copy an electronic database. It may be wise to monitor this issue and decide later whether database protection law should include paper-based databases.

101. The recent Australian case, *Telstra v. Desktop Marketing*, provides an example in which a compiler attempted to assert intellectual property rights (in this case, copyright) in electronic versions of white and yellow page telephone directories. Telstra Corp. v. Desktop Mktg. Sys. Pty Ltd. (2001) F.C.A. 612 (Austl.) (holding that Australian law offers copyright protection for phone books).

102. Feist Publ'ns v. Rural Tel. Serv. Co., 499 U.S. 340, 340 (1991).

103. *Id.* at 349-50.

104. On commercial concerns of American database producers, see Jason R. Boyarski, *The Heist of Feist: Protection for Collections of Information and the Possible Federalization of "Hot News"*, 21 CARDOZO L. REV. 871, 906-08 (1999). Among these is the enactment of the E.U. Directive and the fear that it would not give sufficient reciprocal protection to countries with inadequate database rights. Reichman & Samuelson, *supra* note 9, at 96-97.

105. Brown, Bryan, & Conley, *supra* note 40, ¶ 46.

106. *Feist*, 499 U.S. at 359.

probably thinking in old, paper-based terms. In the digital age, the majority of databases probably fall outside the *Feist* test due to their electronic nature.[107] Therein lies the argument for *sui generis* law that moves beyond the copyright model to protect other interests in compiled information.

3. Private/Personal Databases

Another danger with defining databases too broadly when drafting new laws is catching personal activity in the legislative net. Consider the position of a private individual who creates an electronic database for recording and searching her family tree. Would we expect or want such a database to be protected under a database protection law from unauthorized interference?

Copyright would protect a paper-based family tree as an expressive form. Copyright would also protect the software behind an electronic genealogy database.[108] But would it serve any societal purpose to protect the contents of private information compilations when they are in electronic form? Because individuals are unlikely to commercialize their private databases, the commercial investment rationale for database protection falls away. If an unauthorized third party gains access to the information, the likely harm is not copying, rather interference with privacy. Thus for personal databases, protection should come from privacy law,[109] not from laws protecting the value of commercial databases.

4. Scientific, Technical, and Educational Databases

Removing paper-based and purely personal compilations from the legal definition of a database should not interfere with the aims of legislation protecting the exploitation of commercial databases. More difficult questions, however, arise in relation to databases with significant scientific, technical, or educational applications. Should we also remove these compilations from the definition of database so that no new law can commodify them as intellectual property and remove them from the public domain? Or should we include them in the definition along with permitted

---

107. This is because the value in such compilations is usually in the comprehensiveness of their contents and their non-selectivity. Austin, *supra* note 52, ¶ 58; Brown, Bryan, & Conley, *supra* note 40, ¶ 46.

108. Brown, Bryan, & Conley, *supra* note 40, ¶ 62.

109. In the United States, privacy law remedies for misappropriation of such information may be somewhat lacking. *See* Litman, *supra* note 28, at 1288. However, if the information is stored in a private computer system, there may be remedies available under the common law of trespass. *See* eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

use exceptions in order to protect certain scientific, technical, and educational uses of databases that may become commercialized?

A compromise between these two alternatives may best balance the interests of research and public knowledge against business goals. We can protect the public domain by omitting from the legislative definition of database compilations created purely for scientific, technical, or educational purposes with no underlying intent to commercialize them. Neither the producer nor the user of such a database could assert property rights in the compilation, thus ensuring that the contained information remains free.

By supporting open source licensing provisions, the law could even encourage contractual provisions prohibiting the subsequent commercialization of such database contents.[110] This may be particularly appropriate for databases initially created using government funding, where there are strong policy arguments for leaving such databases in the public domain and prohibiting their subsequent commercialization by parties who were not involved in their creation.

In contrast, information compilations created with multiple purposes—commercial along with scientific or educational uses—merit protection under the rationale I propose for *sui generis* database law. Thus, these compilations should fall under any legislation's definition of database. Once the definition includes such databases, some of the more significant risks to science and education posed by the over-commodification of these databases can be lessened by including exceptions to the prohibited uses.[111] Yet, limiting the definition initially to commercial databases will minimize the need for parties to rely on these exceptions.

Finally, database law should include compulsory licensing provisions that allow those working in science, technology, and education to access and use databases comiled by sole providers of important scientific, technical, and educational material. These difficult questions must be thoroughly debated prior to the enactment of any new legislation.[112]

---

110. These are provisions that restrict future propertization of information subject to the license. For a detailed discussion of open source licensing, see Dennis M Kennedy, *A Primer on Open Source Licensing Legal Issues: Copyright, Copyleft and Copyfuture*, 20 ST. LOUIS U. PUB. L. REV. 345, 347-48 (2001).

111. Government oversight might be useful in policing this; for example, under some kind of dispute resolution mechanism.

112. Hughes, *supra* note 8, at 48-51; Reichman & Uhlir, *supra* note 29, at 799-821 (discussing potential effects of *sui generis* database protection on scientific and technology communities).

5. A Proposed New Database Definition

Given these issues, how should we draft a targeted, robust definition of the databases we wish a new law to protect? One could start with the E.U. Directive approach (involving a relatively generic description of a database), but then except, as a matter of public policy, items that should not be protected under the law.

To achieve the purpose of serving the commercial needs of database producers, the generic part of the definition should include only databases produced with the intention of commercially exploiting them in one or more identified markets.[113] The definition could, for example, begin by extending to all collections of information, facts, or works[114] developed at least partly for commercial exploitation in identified markets. The definition could then exclude: (a) paper-based databases, (b) educational or teaching materials, (c) scientific and technical materials not developed with the intention of commercial exploitation, and (d) compilations developed for private or personal use with no commercial intent.

This approach is similar to the European approach to defining patentable subject matter. The European definition of patentable subject-matter begins broadly[115] and then excludes a list of subject matter not eligible for patent.[116] These exclusions cover subject matter adequately protected by other intellectual property laws[117] and subject matter that should not be protected as a matter of public policy.[118]

Defining databases as compilations created for commercial exploitation in particular markets would link the definition directly to the commercial aims of the legislation. As examined in Part IV, applying such a definition in practice may require registration of the database for use in identified markets and government investigation of a business plan showing how the database will be exploited in these markets. Trademark law provides a basis for drafting such provisions.

---

113. The following discussion takes up the question of how a bona fide intention to commercialize a database in one or more relevant markets might be assessed for the purposes of the legislation and does suggest some government oversight as with trademark and, to some extent, patent law.

114. Such terms could be defined in ways suggested from the E.U. Directive, the Antipiracy Bill, and the Consumer and Investor Access Bill.

115. *See, e.g.*, Patents Act, 1977, § 1(1) (Eng.) (transposing the requirements of the European Patent Convention into domestic English law).

116. *Id.* §§ 1(2) & 1(3).

117. *See, e.g., id.* § 1(2)(b).

118. *See, e.g., id*. §§ 1(2)(a), 1(2)(c), 1(2)(d), 1(3).

A discrete definition will lessen confusion similar to that found in copyright about the proper scope of the fair use exceptions.[119] In particular, it will lessen confusion over whether fair use is a constitutional right or rather a tolerated convenience.[120] By using the definition of database to depart from the copyright model, a new *sui generis* database law can succeed where a copyright-inspired model would fail in protecting the elements of a database that modern commercial database producers seek to protect.[121] This is because limiting the definition of database lessens the need to rely on fair use exceptions to database rights.

Thus, following the European patent law model may be the best way to define databases: (1) strictly limit the concept of a database to those developed for commercial exploitation, similar to registered trademark law; (2) carve out of the definition those elements that are adequately protected by other intellectual property laws or those whose inclusion would be against public policy; (3) amend the list of "carve outs" if the list fails to meet the needs society and commerce. Drafters of an American or an international database protection law should carefully consider this approach.

C. Commercial Exploitation of Databases

Accepting that developing an appropriate initial definition of database is essential for effective database protection laws in the digital age, we must then identify the uses a database creator may want to make of the database and the sort of legal protections these uses may require. This is essential to framing effective and appropriate legislative prohibitions on database use.

Producers must be able to effectively commercialize their information product and clearly set down the contractual rights and obligations of people granted access to the database. Additionally, they must be able to prevent unauthorized access to the database by third parties who have not contracted with them. Legislatures should support any contractual or technological measures used by database producers to achieve these ends as long as those measures do not encroach inappropriately upon any legitimate public interest in free access to information and ideas.

---

119. DAVID, *supra* note 69, at 5-6; LEAFFER, *supra* note 81, at 428.

120. Nimmer, *supra* note 33, at 714-15.

121. There is an associated risk here that any law to protect databases that is too closely modeled on copyright runs the risk of being struck down as unconstitutional. *See, e.g.*, Malla Pollack, *The Right to Know? Delimiting Database Protection at the Juncture of the Commerce Clause, the Intellectual Property Clause, and the First Amendment*, 17 CARDOZO ARTS & ENT. L.J. 47 (1999); U.S. COPYRIGHT OFF., *supra* note 100, at xviii.

Professor Conley summarizes the objectives of a commercial database-producer as follows:

> The objectives of a rationally self-interested database owner will be: (1) to permit authorized persons to use the database fully; (2) to prevent unauthorized persons from using it; and (3) to prevent competitors from copying it in order to create a competitive product. A database owner will judge the adequacy of any form of legal protection according to its capacity to advance these three interrelated objectives.[122]

It may be difficult to produce evidence of a bona fide intention to commercially exploit a database. However, a law confined to protecting only the commercial aspects of databases, rather than protecting compilations of information per se, will have the greatest chance of gaining public acceptance and operating effectively.

Commercial exploitation need not be limited to commercial licensing but may include the database compiler's own uses in commerce. For example, a retail company that collects its customers' spending profiles in a database for use in targeted marketing might be regarded as performing a commercial use.

Contract law may be an appropriate means to deal with some of the above requirements. However, the creation of *proprietary* rights in databases through intellectual property law is also important here but has proven to be more problematic than contracting per se. It is important to legally define the actual proprietary or quasi-proprietary rights of commercial parties so that they may contract effectively with respect to those rights.[123]

Intellectual property rights are also important because contract law cannot always deal effectively with the prevention of unauthorized third party access to database contents. A third party lacking permission to access a database or to use its contents may not be in a contractual relationship with the database maker. Furthermore, even in the situation where a contract exists, the wrongdoer may be acting outside the scope of the contract terms.

When a contracting party uses database content outside the scope of its contract, contractual remedies will be available if the wrongdoer can be identified and made subject to the jurisdiction of a court or other dispute-

---

122. Brown, Bryan, & Conley, *supra* note 40, ¶ 35.

123. As noted by Professor Litman, "The raison d'etre of property is alienability . . . . Property law gives owners control over an item and the ability to sell or license it." *See* Litman, *supra* note 28, at 1295.

resolution forum. However, proprietary remedies may prove to be more meaningful and useful in such circumstances. Certainly, proprietary remedies will be the only useful legal avenue where unauthorized third party access to a database occurs in the absence of a contractual relationship between the parties. For this reason, the discussion now turns to the creation of proprietary or quasi-proprietary rights and remedies in databases.

It should be noted that in the modern technological world, legal protection cannot, and should not, be the only avenue of protection for the contents of electronic databases. Technological protection measures—such as encryption devices, watermarks, and time-limited software mechanisms to prevent unauthorized ongoing use of database contents—should also be employed by database makers to the extent possible and practicable.[124] In many cases, a legal remedy will be less useful than an effective technological measure. The law can only assist efforts taken by parties to protect their information. The law cannot solve all access and use problems, particularly when wrongdoers operate across national borders and evade the laws or jurisdiction of the database maker.[125]

However, there are also practical limitations to pure reliance on technological measures. As noted in a 1999 National Research Council report, "it is almost certain that every technological security method will eventually be able to be countered through the use of other technological advances."[126] Thus, law and technology need to work together to provide adequate protection.

Any new database protection law should support contract and technology protection measures as long as they protect valid proprietary rights in information compilations without interfering unnecessarily with competing public interests. However, when contract or technology protection measures go too far in monopolizing information to the detriment of the public interest, the law should strike down the measure as an unjustified incursion into the public domain.[127]

---

124. PETER N. GRABOSKY & RUSSELL SMITH, CRIME IN THE DIGITAL AGE: CONTROLLING TELECOMMUNICATIONS AND CYBERSPACE ILLEGALITIES 112-13 (1998); NAT'L RESEARCH COUNCIL, *supra* note 55, ch. 3.

125. This has been a problem of copyright protection in the digital age. Even new legislative measures such as the DMCA encounter difficulty in the international arena. Lipton, *Comparative Survey*, *supra* note 33, at 365-69.

126. NAT'L RESEARCH COUNCIL, *supra* note 55, ch. 3.

127. Cohen, *supra* note 65, at 608-09 (on justifications for striking down contract and technological protection measures in the public interest).

Assuming that an appropriate database protection law will confine itself to supporting the reasonable commercial exploitation of databases, the key requirements of database producers may well be those identified by Professor Conley, including the right to: (a) permit authorized persons to utilize database contents; (b) prevent unauthorized persons from accessing or using database contents; and (c) prevent competitors from copying or distributing database contents without authorization. This approach to delimiting relevant rights might be acceptable if the exact boundaries of these rights are clearly defined. In particular, some form of statutory time limit on the exercise of these rights seems important, as does clearly limiting the rights to appropriate commercial uses that do not encroach too significantly into the public domain of information and ideas.

The time limit imposed on the exercise of such rights might be calculated in several ways: (1) based on the amount of time, cost, or effort invested in creating the relevant database; (2) by giving the database creator a reasonable "commercial head start" over its competitors as a reward for its efforts; or (3) on some other basis such as an arbitrary number of years.[128]

III. CRITIQUE OF EXISTING LAWS

Whether or not a new database law ever incorporates the rights listed above, it seems clear that Professor Conley has correctly identified these rights as the aims of a "rationally self-interested database owner."[129] This part of the discussion identifies how current intellectual property laws fail to achieve these aims. It then turns to suggestions for effective database law reform at both the domestic and international levels.

Since 1996, Congress has introduced a number of bills to create some form of database protection system for the United States.[130] However, Congress has yet to reach agreement on the key features of such a new law, particularly the nature and duration of the rights that must be created in databases in order to satisfy the reasonable commercial requirements of database makers. Furthermore, Congress has not agreed on the exceptions

---

128. Wesley L. Austin, *A Thoughtful and Practical Analysis of Database Protection Under Copyright Law, and a Critique of Sui Generis Protection*, 3 J. TECH. L. & POL'Y 3, ¶ 86 (1997) (on file with the author), *available at* http://journal.law.ufl.edu/~techlaw/3-1/austin.html (last visited Aug. 9, 2003); Wolken, *supra* note 67, at 1299.

129. Brown, Bryan, & Conley, *supra* note 40, ¶ 35.

130. For a useful summary of legislative activity in the United States to date, see Brown, Bryan, & Conley, *supra* note 40, ¶¶ 87-91, and Mark Davison, *Proposed U.S. Database Legislation: A Comparison with the U.K. Database Regulations*, 21 EUR. INTELLECTUAL PROP. REV. 279 (1999).

that need to be carved out of those rights to protect legitimate public interests. The approaches to drafting these laws shows the influence of the copyright-based model on commentators and legislators. New laws will not likely be drafted optimally until the debate stops revolving around the perceived failure of copyright to protect databases and begins to focus on balancing the commercial needs of database creators against those of the public at large.

Certainly, any new database protection law must take account of applicable copyright concerns. However, those concerns should be secondary to how the new law itself is modeled. The primary concern should be the underlying conception of a "database" and determining what that term should cover, with an eye towards meeting the real commercial needs of database producers. Given the nature of the information products under consideration and the significant risk of over-commodifying the public domain if regulatory matters are left completely in the hands of the marketplace, the debate should also recognize the need for some level of government monitoring.

The various House bills introduced since 1996 include the following:

1) Database Investment and Intellectual Property Antipiracy Bill of 1996 which closely followed the strongly "proprietary" E.U. model but established a longer (twenty-five-year) period of protection and gave broader rights of exclusion to database makers.[131]

2) Collections of Information Antipiracy Bill of 1997 which also broadly followed the E.U. model but imposed no time limit on protection.[132] This bill allowed some "permitted acts" in relation to a collection of information, but these were regarded by many as insufficient. Originally, these provisions were to be part of what was to become the DMCA, but they were deleted before both houses passed the DMCA in 1998.

3) Collections of Information Antipiracy Bill of 1999 which broadly followed the previous bills but created a new fair use exception to infringement and—in the version as originally introduced—limited the protection period to fifteen years.[133]

131. H.R. 3531, 104th Cong. (1996).
132. H.R. 2652, 105th Cong. (1996).
133. H.R. 354, 106th Cong. (1999).

4) Consumer and Investor Access to Information Bill of 1999,[134] which prohibited the duplication and commercial sale of a database in competition with the original database but did not expressly create proprietary rights in a database[135] and did maintain a significant list of permitted acts[136] in relation to databases.

None of these models has found its way into American law, partly because of disagreements as to how such a law should be drafted and partly because of opposition to all of these approaches from the scientific and technological communities in the United States.[137] These approaches have missed the main issues in this area on which legislators should be focused. All of these bills define databases very broadly, creating potentially far-reaching rights in databases,[138] tempered by vague fair use style exceptions to those rights to balance public and private interests.

A more effective model for database law might clarify points of fundamental importance to the database debate. For example, it is fundamentally important to precisely identify which databases should be regulated and on what basis. It is also crucial that the government effectively monitor the exploitation of database rights in order to prevent the unfettered promotion of commercial activity at the expense of the public interest.

Before considering how these more fundamental issues could be resolved in a model for a new database law, it is necessary to consider the ways in which existing laws fail to strike an appropriate balance between the reasonable commercial needs of database producers and fears regarding the over-commodification of information in the digital age. In so doing, we should keep in mind the aims of database producers in restricting access to databases and preventing unfair commercial competition. Any new database legislation needs to be strictly limited to

---

134. H.R. 1858, 106th Cong. (1999).

135. However, arguably it does so at least by implication. *See* discussion *infra* Part III.C.2.

136. These look somewhat like the fair use exceptions from copyright law. *See* following discussion Part III.A.

137. Hughes, *supra* note 8, at 52-55 (discussing the political and market forces behind the debates for database protection legislation in the United States and in other jurisdictions); Reichman & Uhlir, *supra* note 29, at 823-28.

138. The protected rights under the Consumer and Investor Access to Information Bill are much more limited than those under the various iterations of the Collections of Information Antipiracy Bill. However, I would still argue that the Consumer and Investor Access to Information Bill is overly broad in its definition of database and overly vague in terms of its fair use exceptions to be particularly effective.

meeting these ends without interfering with the broader "intellectual property bargain" in society. Again, we are confronted with the complex problem of balancing private rights against public interests in information. This may be an area where government oversight of relevant laws might be useful in striking an appropriate balance.

A. Copyright

1. Copyrighting Databases: The Feist *Decision*

It is logical to commence this discussion with an examination of copyright law as a vehicle for protecting valuable databases against unauthorized access or use. Copyright was originally regarded as one of the most obvious methods for protecting at least certain types of databases. In most jurisdictions, including the United States and the United Kingdom, copyright law protects a "compilation" or "database" as a "literary work" provided that it meets the statutory requirements for such protection. In England, section 3A(2) of the CDPA provides that a database will be protected in this way if "by reason of the selection or arrangement of the contents of the database the database constitutes the author's own intellectual creation."[139]

In the United States, various provisions of the Copyright Act as interpreted by the courts also similarly protect databases. The copyright subsists in "original works of authorship fixed in any tangible medium of expression."[140] Section 103(a) of the Act acknowledges that copyright protection extends to "compilations" and "derivative works," but this is tempered by section 103(b) which provides that copyright protection extends only to the material contributed by the author of such work and not to pre-existing material employed in the work.

Under United States copyright law, "compilation" is defined in section 101 as:

> [A] work formed by the collection and assembling of preexisting materials or of data that are selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship. The term "compilation" includes collective works.

For the purposes of the definition of "compilation," the term "collective work" is further defined in § 101 as:

---

139. CDPA, § 3A(2). This closely follows the wording of the E.U. Directive, Article 3(1).

140. 17 U.S.C. § 102(a) (2000).

> [A] work, such as a periodical issue, anthology, or encyclopedia, in which a number of contributions, constituting separate and independent works in themselves, are assembled into a collective whole.

Although the terminology and underlying concepts differ slightly, these definitions are clearly related to the concept of a database as defined in the CDPA in England. In particular, there is no direct guidance in the U.S.C. about whether the exertion of time, money, or effort in compiling a database would suffice to trigger copyright protection or whether U.S. copyright law requires a greater degree of originality or creativity. These questions have always been left to the courts in the United States.[141]

The authoritative case on this point is the 1991 Supreme Court decision in *Feist* in which the Court rejected the previously established "sweat of the brow" doctrine as applied to compilations and databases.[142] The "sweat of the brow" doctrine had held that if substantial work had been put into creating a database, this work would satisfy the originality requirements of copyright law.[143] The Court in *Feist* held that the threshold test for acquiring copyright protection in a database is whether there is some originality present in the selection or arrangement of the contents of the database.[144] Evidence of sufficient exertions in creating the database no longer satisfied the originality requirement.

Thus, the plaintiffs in *Feist* could not assert copyright protection for a white pages telephone directory because the Court held that originality was not present in the selection, arrangement, or organization of database content:

> Rural's selection of listings could not be more obvious; it publishes the most basic information–name, town, and telephone number—about each person who applies to it for telephone service. This is "selection" of a sort, but it lacks the modicum of creativity necessary to transform mere selection into copyrightable expression. Rural expended sufficient effort to

---

141. These questions had also been left to the courts in England prior to the transposition of the E.U. Database Directive into national law there in 1997. The definitions of database in the CDPA in England transposed into domestic legislation the judicial tests that have been used in the United States to define the standard of creativity required for copyright protection of a database which had also been adopted in the E.U. Directive. *See* E.U. Directive, *supra* note 27, art. 3(1).

142. Feist Publ'ns v. Rural Tel. Serv. Co., 499 U.S. 340, 363-64 (1991).

143. *Id.* at 352-53.

144. *Id.* at 348.

> make the white pages directory useful, but insufficient creativity to make it original.[145]

In explaining the scope of the originality requirement as applied to databases and compilations, Justice O'Connor noted:

> Originality requires only that the author make the selection or arrangement independently (i.e., without copying that selection or arrangement from another work), and that it display some minimal level of creativity. Presumably, the vast majority of compilations will pass this test, but not all will. There remains a narrow category of works in which the creative spark is utterly lacking or so trivial as to be virtually non-existent . . . . Such works are incapable of sustaining a valid copyright.[146]

Although the *Feist* test is the current approach for ascertaining whether copyright can be asserted in a database in the United States, it has come under criticism both within the United States and elsewhere.[147] It has been suggested that one of the fundamental problems with the *Feist* decision is that it provides no guidance as to what types of databases *will* attract copyright protection in the United States. By setting the standard against a white pages telephone directory—arguably one of the least creative compilations possible—the Supreme Court does not give future courts and commercial entities sufficient guidance as to where the line should be drawn between copyrightable and non-copyrightable databases.[148]

The *Feist* decision also fails to recognize that the value of many computerized databases is in their comprehensiveness. The more information databases contain and the less "selection" they evidence, the more commercially valuable they are likely to become. Such comprehensiveness often requires database makers to exercise minimal selectivity in creating the compilation.[149] This leads to the paradox that the more commercially valuable the database is, the less likely it is to achieve copyright protection.[150] A more selective database is arguably less valuable yet more likely to achieve greater intellectual property protection through copyright.[151]

---

145. *Id.* at 362-63.
146. *Id.* at 358-59.
147. *See* discussion *infra* Part III.A.2.
148. Brown, Bryan, & Conley, *supra* note 40, ¶ 46.
149. *Id.* ¶ 61.
150. *Id.*; *see also* Austin, *supra* note 52, ¶ 58.
151. Wolken, *supra* note 67, at 1278.

Jeffrey Wolken notes that the same problems arise in applying the original "arrangement" criterion to electronic databases to determine copyrightability:

> [I]mposing a definite, physical arrangement on the information contained in a database would severely decrease the database's utility. Even if database producers wanted to gain copyright protection by providing a definite physical arrangement when saving their information, it is not practical for them to do so. In addition to the limitations imposed by the physical process of randomly saving computerized information, any formal arrangement of information would detract from the usefulness of a database. It is the ability of users to search an unrestricted database for the information they want that makes the database valuable. After a search, a user can create for himself the best presentation of the information by imposing his own arrangement on the search results. Generally, the utility of a database is inversely related to the degree of arrangement originally found in the database. More structure equals less utility. Therefore, using "arrangement" as a protectable element of a computerized database is both unfeasible and impractical.[152]

Thus, copyright law in the wake of the *Feist* decision is arguably too thin, failing to protect many databases that are the product of substantial investments of time, effort, and money, but show little creativity in selection and arrangement.[153]

Attempts to protect the value of such databases through other legal measures are also problematic. For example, trade secret law has little application to databases because the way in which a database's information is commercialized often makes it difficult to keep the information secret.[154] Furthermore, a database that is not sufficiently original to attract copyright protection will almost certainly not satisfy patent law's novelty and non§obviousness requirements.[155]

Contract protection is also problematic. First, the wrongdoer may not be in a contractual relationship with the database maker.[156] Second, even if there is a contractual relationship, the database maker may be unable to obtain assent to restrictive contractual clauses limiting the permitted uses

---

152. *Id.* at 1277-78.

153. Brown, Bryan, & Conley, *supra* note 40, ¶ 70.

154. MANN & WINN, *supra* note 61, at 377.

155. 35 U.S.C. §§ 102-103 (1994).

156. It may be that concepts of implied contract may be useful here in some situations.

of database contents. Obtaining such assent may also be inconsistent with the database maker's business objectives.[157] Third, some still the question the validity and enforceability of clickwrap licenses relating to contractually permitted uses of information[158] despite some judicial[159] and legislative[160] support for such terms. Fourth, jurisdictional problems may prevent the enforcement of such terms, particularly where the alleged wrongdoer is located interstate or overseas from a database producer.[161] Finally, in online commerce, a complainant database producer may not be able to find or identify a contracting party who has breached contract terms—an issue obviously not unique to contract law.

The *Feist* copyright protection standard fails to meet a database producer's key objectives as identified by Professor Conley. The standard fails to allow *any* rights in a database that lacks sufficient originality in the selection or arrangement of its contents. Therefore, the *Feist* standard will exclude copyright protection for many valuable commercial databases.[162]

2. International Criticism of the Feist *Decision:* Telstra v. Desktop Marketing Systems

The *Feist* decision has also attracted critics outside the United States. In the recent Australian Federal Court case of *Telstra Corp. v. Desktop Marketing Systems*[163], Judge Finkelstein criticized the U.S. position. In *Telestra*, Judge Finkelstein was ruling on a factual situation very similar to *Feist*, except the *Telstra* case involved electronic versions of what were paper-based telephone directories in *Feist*.[164]

In *Telstra*, Desktop Marketing Systems reused without permission significant amounts of information contained in Telstra's white pages and yellow pages directories. Judge Finkelstein held that Telstra could assert copyright in both its white and yellow page directories.[165] The selection

157. Brown, Bryan, & Conley, *supra* note 40, ¶¶ 39, 70.

158. Madison, *supra* note 38 at 1117-19.

159. ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1447 (7th Cir. 1996).

160. For example, UCITA has been enacted to date in several States including Maryland and Virginia. *See* in particular U.C.I.T.A. § 112 (2001).

161. It should be noted that with information commerce in the digital age, this problem is not limited to contract law.

162. RADIN, *supra* note 49, at 763.

163. (2001) F.C.A. 612 (Austl.).

164. This fact may lend weight to the point that it is really electronic commerce that requires the protection of any new database laws, and that there may be good reasons to exclude paper-based databases from their reach. *See id.*

165. The Australian Federal Court of Appeal upheld Judge Finkelstein's first instance decision in the case. Desktop Mktg. Sys. v. Telstra Corp. (2002) F.C.A.F.C. 112 (Austl.). Moreover, because the High Court of Australia has recently refused leave to appeal the

and arrangement of the contents showed sufficient originality to attract copyright protection.

In considering Desktop's arguments citing the *Feist* decision, Judge Finkelstein suggested that Justice O'Connor in *Feist* may have been incorrect when she said that limiting copyright in compilations to those where there has been an exercise of judgment will not affect many publications.[166] The *Feist* decision's outcome is that many obvious methods of grouping or listing data—for example, alphabetically, chronologically, or sequentially—will be denied originality even though the obviousness of the selection and arrangement may give the database its value.[167] Judge Finkelstein suggested that the *Feist* court made a mistake when it assumed that its ruling would be limited only to those circumstances in which originality would not be found in a database.[168]

Judge Finkelstein also noted that *Feist* has caused much confusion in subsequent cases in the United States dealing with various yellow page telephone directories.[169] This implied that it would be imprudent for Australia to embrace law that could cause similar problems in future cases. Judge Finkelstein then weighed the practical advantages and disadvantages of following a similar rule in Australia and concluded that:

> There are policy reasons both for and against the result in *Feist* . . . . On the one hand, the ability to prevent others from appropriating information in a compilation of facts will severely limit the ability of later authors to build upon earlier works. This may impair progress in both the sciences and the arts . . . . On the other hand, there are those who argue that the abandonment of the "sweat of the brow" theory has threatened the progress of information. The argument is that the collection of factual

---

decision, the Full Court Decision will stand as the current law in Australia. *Result of Applications for Special Leave to Appeal*, High Court of Australia (June 20, 2003), *at* http://www.hcourt.gov.au/registry/slresults/20-06-03M.htm

166. Feist Publ'ns v. Rural Tel. Serv. Co., 499 U.S. 340, 358-59 (1991).

167. *Telstra*, F.C.A. 612 at ¶ 74.

168. *Feist*, 499 U.S. at 358-59. In fairness, we must remember that *Feist* was decided in the early 1990s, prior to the rise of electronic databases as a major worldwide commercial industry.

169. *Telstra*, F.C.A. 612 at ¶¶ 76-79. Judge Finkelstein also discusses relevant Canadian case law in a similar vein to *Feist*. *See, e.g.*, Tele-Direct Inc. v. Am. Bus. Info. Inc., [1997] 154 D.L.R. 4th 328 (Fed. Ct.) (Can.) (holding that copyright did not subsist in a yellow pages directory because the publisher had exercised only a minimal degree of skill or judgment in the overall arrangement of the publication which was insufficient to support a claim for originality). The fact that there was industrious collection of the information was not regarded as relevant. *Id.*

> material is essential to the economy. Databases provide a wealth of information to business people, professionals, scientists and consumers. If copyright protection is not given, the investment of the time and money that is required to produce these compilations will not be forthcoming.[170]

The answer to the problems listed by Finkelstein may be to extend copyright protection to databases where a substantial investment has been made in their creation, but there may be a better alternative. England, for example, has recently replaced the "sweat of the brow" theory of copyright protection for compilations and databases with a *sui generis* database right for databases whose selection and arrangement do not meet originality requirements of copyright. Of course, copyright is still available in England for those databases that meet the originality criteria.[171] These developments are largely the result of the requirement that English law comply with the E.U. Directive of 1996, discussed in the next section.

The English and E.U. laws create overly broad new *sui generis* intellectual property rights in databases that are too closely based on copyright concepts and go well beyond the reasonable needs of commercial database producers.[172] However, these laws do show that many parts of the world do not regard copyright protection as a sufficient or appropriate way to protect the commercial value of electronic databases. The drafting of a number of database protection bills within the United States[173] shows similar concerns.

Even those who criticize both the E.U. and U.S. approaches are not unsympathetic to the conundrum described by Judge Finkelstein. In the introduction to their seminal article on database protection in the United States, Professors Reichman and Samuelson stated:

> The Authors of this Article are not unsympathetic to many of the goals that the sui generis database regimes are meant to achieve. We have elsewhere argued that the traditional intellectual property models, as supplemented by trade secret laws, often fail to afford those who produce today's most commercially valuable information goods enough lead time to recoup their investments. The risk of market failure inherent in this state of chronic under-

---

170. *Telstra*, F.C.A. 612 at ¶ 83.

171. CDPA, *supra* note 80, § 3A.

172. Reichman & Samuelson, *supra* note 9, at 84-95.

173. See the discussion *infra* Part III for details of the various bills drafted in the United States to date.

> protection tends to keep the production of information goods at suboptimal levels.[174]

Although ultimately rejecting the suggestion that the United States should adopt a database right like that now available in the European Union, Professors Reichman and Samuelson suggest that there should be some additional form of protection for databases based on a different model.[175]

3. Limitations of Copyright Law in the Database Context

Having surveyed the different approaches to copyrighting databases in various jurisdictions, copyright clearly is not the most appropriate way to protect the commercial value of many databases, notably electronic databases. Even absent the concerns raised about copyright law's inability to protect unoriginal databases, the policies underlying copyright law are not appropriate for commercial database protection.

In jurisdictions and circumstances where copyright protection is available for databases, the copyright protection will arguably be greater than necessary.[176] Even though such protection might provide incentives encouraging the production of databases, the ensuing protection may stifle development of products that compete with those databases. Development might be stifled even for products that would not directly compete in the same market but which used existing database content in a different field.[177]

Although created as private property rights by statute, copyrights in most jurisdictions are largely exploited and enforced under market control. As argued previously and taken up further in the following discussion, the creation and exploitation of private property rights in databases may require a higher degree of government oversight than currently exists under copyright law.

Even if a "sweat of the brow" doctrine for copyright protection of databases were accepted across many jurisdictions,[178] is this really what copyright law was designed to protect? Although there is a significant history of "sweat of the brow" cases being upheld in jurisdictions such as

---

174. Reichman & Samuelson, *supra* note 9, at 55.

175. *Id.* at 137-63.

176. This is even more so when the "sweat of the brow" doctrine is accepted as the basis for copyright protection (as it is in some jurisdictions like Australia), and a broader range of databases are potentially protected as copyrightable works.

177. Reichman & Samuelson, *supra* note 9, at 125-26.

178. This seems unlikely to happen in practice, particularly in jurisdictions such as the United States.

the United States (pre-*Feist*), the United Kingdom (prior to the E.U. Directive) and Australia, this history may have been underscored by policy concerns on the part of judges that defendants should not "reap where they have not sown," and that copyright should come into play to prevent such appropriations in the absence of any other effective form of intellectual property protection for databases and compilations. Thus, it may be preferable to develop new rights tailored to commercializing valuable databases.

Copyright law is about expression, not about ideas.[179] Copyright in a database should not extend protection to the database's valuable elements—the facts and information contained therein.[180] Yet, the indirect effect of the "sweat of the brow" doctrine may have been to extend copyright in this direction.[181] This is another argument for removing the "sweat of the brow" doctrine from copyright law, as *Feist* effectively did in the United States.

Copyright law was created and structured to protect artistic rights,[182] not commercial rights, even though it has been used to protect commercial activities.[183] Rather than pulling copyright law further towards commercial and non-artistic objectives, legislatures should create a new law with clearly commercial aims and structures that deals with the commercial exploitation of databases.[184]

Because a copyright in a database or compilation protects only the selection and arrangement of the contents of the database,[185] a producer of a second database could avoid copyright infringement by copying only facts from a copyrighted database rather than expression of these facts. For

---

179. BOUCHOUX, *supra* note 74, at 146.

180. Austin, *supra* note 52, ¶ 1.

181. *See* Wolken, *supra* note 67, at 1273-75.

182. BOUCHOUX, *supra* note 74, at 133-38. However, it should be noted for completeness that much of early English copyright law was based on commercial imperatives related to the publishing industry, and that the United States clearly followed this tradition. *See* W.R. CORNISH, INTELLECTUAL PROPERTY: PATENTS, COPYRIGHT, TRADE MARKS AND ALLIED RIGHTS, ch. 9 (4th ed. 1999).

183. An obvious example is the reliance by movie studios on copyright, and on the recently enacted provisions of the DMCA, to protect property rights in movies released on DVD for public sale. This was the basis of the litigation in *Reimerdes*. Universal City Studios Inc. v. Reimerdes, 111 F. Supp. 2d 294, 344-45 (S.D.N.Y. 2000).

184. As noted above, the new law could be modeled more directly on concepts derived from patent and trademark laws to the extent that they focus more clearly on creating commercial intellectual property rights, rather than artistic rights that are based on the prevention of copying.

185. CDPA, *supra* note 80, § 3A(2); Feist Publ'ns v. Rural Tel. Serv. Co., 499 U.S. 340, 348 (1991).

examples, a second producer could rearrange the database contents into a different format, which is inexpensive and easy to achieve with digital technologies.[186]

Copyright law will continue to protect certain aspects of some databases in many jurisdictions, including the United States, the European Union, and Australia. Yet there is no international consensus that copyright is the most appropriate way to protect a database's commercial value. In fact, the consensus is that copyright is clearly an inappropriate vehicle for many of the reasons described above. For example, copyright is clearly inappropriate for broad comprehensive electronic databases whose value lies in their coverage and ease of searching, rather than their originality in selection or arrangement of information. For this reason, copyright law is not a long-term solution to the commercial needs of modern electronic database producers.

B. Trade Secrecy

1. Basis of Trade Secret Law

Trade secret protection has a much more limited application to databases than copyright law.[187] In the United States, trade secret law is a body of both state and, more recently, federal law[188] that protects the value

186. Wolken, *supra* note 67, at 1279-80.

187. It should be noted that trade secret law is the only aspect of state law from the United States considered in this discussion. This is because it is the most relevant part of state law to the discussion of the protection of information contained in a commercially valuable database. For completeness, it should be noted that there are some other parts of state law that may have some relevance in the database context, although they are even more vague and arguably of more questionable application in this context than trade secret law. They have thus been omitted from this discussion. The most notable such area of state law, potentially relevant to protecting facts and ideas that are not otherwise protected by patent or trade secret law is the somewhat vague and non-uniform "misappropriation" doctrine based on the Supreme Court case of *International News Service v. Associated Press*, 248 U.S. 215 (1918). Although no longer part of the federal common law, the doctrine has arguably survived in state law in at least some states and may apply to situations where a person has invested substantially in the creation of a valuable intangible item relating to information that is not otherwise protected by patent or trade secrecy, and where a second person has appropriated his or her idea as a free rider at little cost, thereby injuring the original developer. State courts will sometimes grant injunctions or award damages in such circumstances to counter the effect of free-riding on the original developer of the intangible product. This doctrine has been severely criticized and is very rarely raised in litigation in practice. The doctrine is arguably pre-empted by federal patent and copyright law, which is why no space has been devoted to it in the main text. *See* LEAFFER, *supra* note 81, at 41-43; Boyarski, *supra* note 104, at 871; Brown, Bryan, & Conley, *supra* note 40, ¶¶ 39-40.

188. Economic Espionage Act, 18 U.S.C. § 90 (1996).

of information kept out of the public domain through secrecy and obligations of confidence.[189] Comparable doctrines have developed in other countries.[190]

The ability of trade secrecy to protect valuable commercial information that is not particularly novel or creative is an advantage over other intellectual property law. Specifically, when compared to patent law, trade secrecy (a) protects a potentially broader array of non-novel information, such as customer lists and marketing plans;[191] and (b) does not require patent law's high standards of inventiveness.[192] Because of these advantages, some businesses choose to rely on trade secret protection rather than patent protection. This is especially true where the information in question is not novel, inventive, or the information's value does not justify the time and expense of seeking a patent.[193]

In fact, even where an invention would be patentable, many businesses choose to keep it secret because they can then obtain a much longer period of protection than a patent's twenty-year term.[194] For example, Professor Leaffer notes that for business processes such as the formula for Coca-Cola trade secrecy is more attractive than a patent.[195] Trade secrecy allows a few people to practice the invention in secret, particularly where reverse engineering of the invention is difficult.[196] The trade secret lasts as long as substantial secrecy can be maintained.[197]

The United States likely has the most well-developed trade secret laws in the world.[198] The United States has legislation designed along a torts model to prevent and redress misappropriations of trade secrets.[199] Other jurisdictions, such as the United Kingdom, have relied more heavily on doctrines derived from the common law and equity, such as breach of

189. Lynn Sharp Paine, *Trade Secrets and the Justification of Intellectual Property: A Comment on Hettinger*, 20 PHIL. & PUB. AFF. 247, 250-51 (1991).

190. *See* Lipton, *Commercial Information*, *supra* note 54, at 9-15.

191. LEAFFER, *supra* note 81, at 37.

192. *Id.*

193. *Id.*

194. 35 U.S.C. § 154(a)(2) (2000).

195. LEAFFER, *supra* note 81, at 38.

196. *Id.*

197. *Id.*

198. For an overview of trade secret law, see BOUCHOUX, *supra* note 74, ch. 22. *See also* James Hill, *Trade Secrets, Unjust Enrichment, and the Classification of Obligations*, 4 VA. J.L. & TECH. 2, 6 (1999); Lipton, *Commercial Information*, *supra* note 54, § 2.1.

199. *See, e.g.*, UNIF. TRADE SECRETS ACT (amended 1985); Federal Economic Espionage Act, 18 U.S.C. § 90 (1996); Ruckelshaus v. Monsanto Co., 467 U.S. 986 (1984).

contract and breach of confidence, to protect valuable commercial confidences.[200]

The main difference between these approaches is that the United States courts and legislatures have treated trade secrets as a form of property[201] that is capable of being appropriated by a wrongdoer. In contrast, lawmaking bodies in most other jurisdictions, rather than treating information as the misappropriated property of the victim, base remedies on the nature of the relationship between the parties.[202] This latter approach is difficult to apply to third party misappropriations of valuable information where the victim and the wrongdoer lack any contractual or equitable relationship.[203]

However, although U.S. trade secret law seems to protect proprietary, rather than purely contractual, interests, it may be more similar to the law in some other jurisdictions than it might first appear. As Professor Leaffer has noted:

> Trade secrets have the attributes of property, and can be licensed, taxed, and inherited. But if an attribute of property is the right to exclude others from using it, the trade secret is a weak form of property protection. A trade secret can only be enforced against improper appropriation, such as theft by an industrial spy, or a breach of a confidential relationship not to divulge the trade secret. This is why it is often said that trade secret [sic] protects a *relationship* rather than a property interest.[204]

Thus, the main advantage of the American legal approach to trade secrecy may be that trade secrets can be more easily dealt with as property in a transactional sense[205] than is possible in other jurisdictions. This is because the United States has accepted the "property" label. In other jurisdictions, such as the United Kingdom, a trade secret is, at best, labelled "quasi-property."

---

200. *See*, *e.g.*, CORNISH, *supra* note 182, at 301-06.

201. *Ruckelshaus*, 467 U.S. at 1002.

202. *See* Lipton, *Commercial Information*, *supra* note 54, § 2.1.

203. JILL MCKEOUGH & ANDREW STEWART, INTELLECTUAL PROPERTY IN AUSTRALIA, 85-86 (2d ed. 1997).

204. LEAFFER, *supra* note 81, at 38 (emphasis added); *see also* NIMMER, *supra* note 37, ¶ 3.02[1]; Paine, *supra* note 189, at 256-58. Professor Litman has also noted that a proprietary label is often attributed to information to ensure ease of transferability/alienation of the information, despite the fact that property theory is generally not a good basis for explaining legal rights in information. *See* Litman, *supra* note 28, at 1283.

205. *Id.* at 1296.

2. The Secrecy Requirement

The question of just how *secret* a trade secret must be to acquire legal protection is important to the present discussion. As Professor Leaffer notes, *absolute* secrecy is not required, but the more widely the information is used in the relevant industry, the less likely it can be protected as property.[206] In determining trade secrecy, courts will take into account: (a) the extent to which the trade secret holder's employees know the subject matter,[207] and (b) the extent of measures taken to guard the subject matter's secrecy.[208]

These factors significantly limit the relevance and usefulness of trade secret law to protect the content and constituent software of commercially valuable databases.[209] The whole point of a database is to make content available, usually for a fee, to members of the public who are not necessarily limited to a particular industry. Although contracts can be used to limit the end-user's use of the content and to maintain some secrecy, these contracts face the drafting and enforcement problems outlined above.

Courts are unlikely to find that materials intended for broad dissemination meet the requisite secrecy. This is so, even if the materials are disseminated for a fee and protected by confidentiality clauses that limit the end-user's uses of the data.[210] Furthermore, in this context, customer confidentiality clauses may be suspect if obtained through a "shrinkwrap" or "clickwrap" license. The plaintiff's customers may not read the license, and such licenses are still of questionable enforceability despite the enactment of UCITA in several jurisdictions within the United States.[211]

There have also been significant concerns raised about the effectiveness of trade secret law to protect computer software that is distributed to the public. Software components of a database made

206. LEAFFER, *supra* note 81, at 38.
207. *Id.*
208. *Id.*
209. *See* MANN & WINN, *supra* note 61, at 377.
210. *Id*.
211. *See also* Ajay Ayyappan, *UCITA: Uniformity at the Price of Fairness?* 69 FORDHAM L. REV. 2471, 2493-95 (2001); Ingrid Michelsen Hillinger, *Consumer Protection Rules In and Around the Uniform Computer Information Transactions Act*, 649 PLI/PAT 401, 405-08 (2001); Carlyle C. Ring, Jr., *UCITA: Contract Rules for Information Commerce*, 649 PLI/PAT 45, 50-51 (2001); Michael L. Rustad, *Making UCITA More Consumer-Friendly*, 18 J. MARSHALL J. COMPUTER & INFO. L. 547, 578 (2000).

available to the public are vulnerable to reverse engineering. Trade secret, like copyright, law permits reverse engineering provided that access to the software was not obtained illegally.[212] In many cases, database content can also be discovered by reverse engineering the software, or simply through computer hacking.[213]

For the above reasons, trade secret law will likely have limited application or usefulness in protecting databases from unauthorized access, use, and disclosure. That trade secrecy law is far from uniform internationally and within the United States simply compounds the problems. For example, not all U.S. states have adopted the Uniform Trade Secrets Act and those that have, have not enacted it uniformly.[214] This non-uniformity within the United States will not be solved by the enactment of the Economic Espionage Act in 1996 as a federal criminal law dealing with trade secret misappropriation. This federal statute creates new criminal penalties for trade secret misappropriation but does not pre-empt non-uniform state law in state civil court cases.[215]

The federal criminal legislation will prove useful (and indeed has already proven useful) in many cases of trade secret misappropriation because the victim of a misappropriation will save time and money by having the government pursue the offender. However, disadvantages include the potential lack of monetary remedy for the victim. And federal prosecutors may not pursue database cases, particularly if they foresee problems with defining database contents as trade secrets for the reasons identified above.

International trade secret law is also far from uniform. As noted above, courts in jurisdictions such as the United Kingdom have based their protection of valuable commercial confidences on the law of contracts and breach of confidence,[216] despite calls from the Law Commission to enact specific trade secret legislation.[217] Other jurisdictions throughout the European Union have taken varied approaches to the legal protection of

---

212. *See*, *e.g.*, LEAFFER, *supra* note 81, at 109; Reichman & Samuelson, *supra* note 9, at 59-60.

213. LEAFFER, *supra* note 81, at 109.

214. *See* Nat'l Conference of Commissioners on Uniform State Law, *A Few Facts About the Uniform Trade Secrets Act*, (on file with the author), *available at* http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-utsa.asp (last visited June 18, 2002).

215. 18 U.S.C. § 1838 (1996).

216. *See* CORNISH, *supra* note 182, at 301-07.

217. LEGISLATING THE CRIMINAL CODE: MISUSE OF TRADE SECRETS (UK Law Commission, Consultation Paper No. 150, 1997), *available at* http://www.lawcom.gov.uk/351.htm.

trade secrets despite the fact that the aim in each case is to protect the value of commercial information where all efforts have been made by its "owner" to retain secrecy.[218]

Because of trade secrecy law's national and international divergence and at its inherent shortcomings at protecting databases, trade secret protection is unlikely to be the solution to the problems faced by digital database makers. An alternative form of protection is necessary.[219]

C. *Sui Generis* Database Protection Laws: Property Versus Tort

1. Existing Approaches to Sui Generis *Database Legislation*

Many scholars have recognized the need for a new form of database protection law outside of contract, patent, copyright, and trade secret laws.[220] While Professors Reichman and Samuelson criticized early attempts at drafting *sui generis* database protection legislation, they agreed that there was a need for new approaches to the issue because existing laws failed to address the realistic commercial needs of database producers.[221]

Accepting, as many scholars do, that there is some need to create a legal approach to protecting commercially valuable databases as a form of property or quasi-property,[222] the question then becomes "what form should such a law take?" To date, the debate has focused on two broad approaches to database protection. The first, the "property model," involves the protection of valuable database contents under a new form of

---

218. Brown, Bryan, & Conley, *supra* note 40, ¶ 77.

219. It is interesting that the enactment of the Electronic Espionage Act in 1996 might be evidence of the need for enhanced government monitoring and regulation of information property rights, albeit through the criminal justice system in this case. Clearly domestic and international market forces were not ultimately regarded by Congress as sufficient to regulate the exploitation and dissemination of valuable trade secrets, particularly in international commerce.

220. *See, e.g.*, Hughes, *supra* note 8, at 86-98; Reichman & Samuelson, *supra* note 9, at 137.

221. Reichman & Samuelson, *supra* note 9, at 137.

222. *Id.*; *see also* Austin, *supra* note 52, ¶ 63; Dennis S. Karjala, *Misappropriation as a Third Intellectual Property Paradigm*, 94 COLUM. L. REV. 2594, 2594-95 (1994); Wolken, *supra* note 67, at 1268-70. However, it should be noted for completeness that there are those who have raised arguments against database protection citing in support of this view issues such as: (a) the fact that the information industry is growing dramatically under the present system; (b) because of the pace of technological change, any new legislation could be obsolete before it took effect; and, (c) the undesirability of commodifying information and limiting free access which has, until recently, been the cornerstone of the digital revolution. *See* Austin, *supra* note 52, ¶¶ 60-61; Brown, Bryan, & Conley, *supra* note 40, ¶¶ 95-110.

intellectual property right that grants *proprietary* protection over database contents.[223] The second approach, the tort/misappropriation model, bases the protection of a database's inherent value on the economic impact caused by a second-comer in a market "free riding" on the work of the original database producer.[224] This approach aims to prevent unfair conduct in a market without expressly creating "property rights" in database contents.[225]

The distinction between the two models is somewhat spurious. By definition, the tort/misappropriation model implies some sort of property rights, even if the rights are weaker or less absolute than those contemplated under the property model. For example, U.S. trade secret law uses a tort/misappropriation approach to protect the value of commercial information.[226] However, this law also clearly involves property rights. Although legislation does not necessarily describe trade secrets as property, it implies that trade secrets are a form of intangible intellectual property.[227] It is impossible to have a tort law based on misappropriation of property without accepting in the first place the existence of the property.

A debate that focuses on choosing between these two approaches is fruitless, and will likely only lead to inadequate draft legislation like that now being debated in the United States.[228] The main distinctions between the two approaches are the duration of a database's legal protection and the basis for calculating database infringement damages. These issues are important but not as fundamental to the development of new law as recognizing the appropriate foundations of the law from first principles, in terms of precisely what interests are being protected and on what basis. Once the basic foundations of a new law are established and its structures

---

223. An example is the United Kingdom's adoption of the principles of the E.U. Database Directive. A broad "personal property" right is expressly created in The Copyright and Rights in Databases Regulations, (1997) SI 1997/3032, R. 13(1) (Eng.).

224. *Id.*

225. Reichman & Samuelson, *supra* note 9, at 137-63.

226. *Id.* at 60-61.

227. The terms "property" and "property right" do not appear in legislation such as the Uniform Trade Secrets Act and Economic Espionage Act, 18 U.S.C. §§ 1831-1839 (1996). However, the legislation clearly contemplates "ownership" of legal and equitable interests. See, for example, the definition of "trade secret" in 18 U.S.C. § 1839(3)-(4).

228. Both the Antipiracy Bill and the Consumer and Investor Access Bill arguably owe too much to their origins in copyright law to be effective in the database context, even though the former may be described as a "proprietary" model and the latter as a torts/misappropriation model. The following discussion explains why these approaches are not satisfactory and suggests directions for law reform in this area that diverge from the approaches taken in these bills.

clarified, it is relatively simple to create appropriate terms of protection and damage calculations to meet the needs of the market, and of society, at the relevant time.

Because both models involve the commodification of databases as property to some degree, fears about over-commodification of information beyond the reasonable needs of commercial database producers may arise. It is more important, however, to ascertain with a focus on relevant commercial activities the extent to which databases can and should be commodified.

The property versus tort/misappropriation debate might help inform the secondary debate on periods of protection and calculation of damages. However, the debate does not resolve the primary questions regarding the appropriate foundations of a new legal system for databases. Clearly, property rights in information compilations will be part of any new legislative package, whether expressly or by implication. What is important, however, is working out how to create, tailor, and monitor rights appropriately to meet the needs of the information society.

2. The Consumer and Investor Access to Information Bill

To date, examples of both the tort/misappropriation approach and the proprietary model for database protection legislation have been drafted. The E.U. Directive, which is discussed in the next section, is a clear example of the proprietary approach, and several draft United States database laws are modeled on this law. The only existing model of database protection legislation that uses the tort/misappropriation approach is the Consumer and Investor Access Bill.[229] The Consumer and Investor Access Bill has never become law. However, despite its unenacted status, it is a useful example of the approach commentators have had in mind when describing a tort/misappropriation model for database protection legislation.

The Consumer and Investor Access Bill defines database broadly, as described in Part I. However, in contrast to the proprietary approach, it does not expressly create proprietary rights in a database. It prohibits the public sale or distribution of a database that (1) duplicates another database collected and organized by another person, and (2) is sold or distributed "in commerce in competition with" the original database.[230] Although no express proprietary right in a database is created here, an implied proprietary or quasi-proprietary right is arguably created. The

229. H.R. 1858, 106th Cong. (1999).
230. *Id.* § 102.

Consumer and Investor Access Bill's underlying assumption is that when a competitor wrongfully misappropriates the property of a database maker, that competitor should be required to compensate the database maker for resulting economic loss.

The Consumer and Investor Access Bill's prohibited activities are tightly restricted to sale or distribution in competition with the original database. This is a significant step towards restricting the reach of *sui generis* database protection law to reasonable commercial activity. The prohibition extends to sale and distribution of "duplicates of a database," connoting a database that duplicates a substantial part of another database.[231]

The bill does not prohibit duplication or copying per se of the database contents, which distinguishes this law from the copyright model.[232] However, it does carve out fair use exceptions that appear to have been modeled on copyright law. These exceptions include "permitted acts" relating to independent collections of information;[233] news reporting;[234] law enforcement and intelligence activities;[235] and scientific, educational, or research activities.[236]

Thus, even though the Consumer and Investor Access Bill is drafted according to the tort/misappropriation model and addresses some of the concerns about database protection, it probably depends too much on copyright law to effectively balance the needs of database producers against public policy concerns.

The more database protection law relies on vague copyright concepts like "fair use" and "permitted exception" provisions, the more room there is for difficult questions regarding coverage of the law to arise.[237] Courts

---

231. "Duplicate" is defined in the bill as connoting a database that is "substantially the same" as the original database and was "made by extracting information" from the original database. *Id.* § 101(2).

232. In any event, it is appropriate that copying of database contents not be proscribed under any new law. This issue is taken up in more detail below.

233. H.R. 1858 § 103(a).

234. *Id.* § 103(b).

235. *Id.* § 103(c).

236. *Id.* § 103(d). There are further exclusions from the scope of the prohibition set out in section 104 relating to government information, databases related to effective Internet communication, computer programs, ideas, facts, procedures, systems, concepts, methods of operation, principles, discoveries, and subscriber list information. *See id.* § 104.

237. However, it might be argued that many of the fair use exceptions in the Consumer and Investor Access Bill would not be likely to come into play in practice if the Bill was ever enacted into law. This is because most of the exempt uses are not likely

have difficulty determining the scope of fair use exceptions and often rule inconsistently.[238] For this reason, exceptions should not be too heavily relied upon in any new database law. Greater legislative guidance on the initial limitations of the rights in question will minimize the need to focus on fair use exceptions because fewer cases will arise on these exceptions if the rights in question are more tightly restricted in the first place.[239]

Obviously, any *sui generis* database protection law must rely to some extent on exceptions to prohibited conduct. However, the more these exceptions are simplified by tightly restricting the concept of a protected database, the more efficient the operation of the legislation will be. It is thus necessary to have a clear and easily discernible relationship between the definition of database and any prohibited conduct involving databases.

The Consumer and Investor Access Bill quite satisfactorily limits the scope of the prohibitions to certain commercial activities. However, broadly defining "database" and then prohibiting clear-cut activities involving databases is not the same thing as tightly limiting the definition of a database initially and then clearly relating the definition to the prohibitions. The latter approach focuses the legislation much more effectively on a limited range of information products from the beginning. The permitted activities involving those databases are also automatically limited because of the more restricted scope of database definition.[240]

3. The E.U. Approach

The E.U. Directive is the only model of *sui generis* database legislation that has been enacted in any jurisdiction. The E.U. Directive is purely a proprietary rights model that expressly creates broad, generic rights in the exploitation of database contents, then carves out some fair

---

to be in commercial competition in any event, and are therefore unlikely to infringe the main prohibition in the first place. On another point, it should also be noted that there are some additional problems with the Consumer and Investor Access Bill as currently drafted, not the least of which is § 106(b) which deals with limitations on liability where a database owner is said to have "misused the protection" afforded by the legislation, with some broad general guidance as to how the concept of "misuse of protection" is to be defined.

238. DAVID, *supra* note 69, at 14-15; LEAFFER, *supra* note 81, at 428.

239. In other words, the legislative grant of lesser rights must, by definition, give rise to less litigation about the scope of those rights. This is particularly the case if the assertion of a right requires registration, supported by documentation that is investigated by an expert body of administrators.

240. As suggested in the early part of this discussion, the concept of database could be limited in the definition section of any new legislation expressly to exclude things like: (a) paper-based databases, (b) databases developed primarily for educational, scientific, or technological use, (c) databases developed primarily for personal use, etc.

use exemptions from liability. As set out below, there are many problems with this model. However, it should be kept in mind that a tort/misappropriation model may generate many of the same problems.[241]

The European Union's original plan was more akin to a tort/misappropriation model that protected databases to prevent free riding in the database industry by competitors who unfairly extracted database contents.[242] Early versions of the E.U. Directive also included provisions requiring compulsory licensing of databases that were the sole source of certain information within an industry.[243] These provisions were designed to give database makers the head start they deserved for being the first players in the market, while allowing others to enter the market at a reasonable market cost. The provisions were not originally designed to give the database maker an exclusive property right in the fruits of its labors.[244] However, determined lobbying by those in favor of protectionist strategies for the global information infrastructure—publishers and some E.U. and U.S. officials—successfully transformed the original E.U. proposal from "a relatively weak liability regime to a strong exclusive property right."[245]

4. The Current E.U. Framework As Adopted in the United Kingdom

The final version of the E.U. Directive shows the advantages and disadvantages of its approach to *sui generis* rights in databases. Examining the operation of the Directive throughout the European Union, Professors Reichman and Samuelson have expressed various concerns:

1) The final version of the E.U. Directive moves away from notions of unfair or unauthorized uses of database contents, instead favoring the exclusive right of database makers to prevent

---

241. This is why the thrust of this Article is to suggest some new approaches to the question of database protection legislation, rather than to enter the debate about whether or not property rights should be created in databases.

242. *See* Reichman & Samuelson, *supra* note 9, at 80-82.

243. *Id.* at 82. Sole source information providers are likely to raise difficult issues whatever form of law is ultimately enacted in any jurisdiction. It is arguable that however any new law is framed, it *must* contain specific provisions that deal adequately with these issues to prevent commercial monopolies of information that should be accessible in the public domain. The appropriate mechanism to deal with this may well be compulsory licensing, perhaps with determinations of the need for licensing in a particular case, and appropriate amounts of royalties to be determined by a specially constituted body of experts in the field. This could be set up under any new legislation.

244. *Id.* at 80-83.

245. *Id.* at 75-76, 84.

extraction and re-use of a substantial part of a database's contents (evaluated quantitatively or qualitatively).[246]

2) The Directive's fifteen-year term for the property right in a database can apparently be indefinitely extended.[247]

3) The Directive does not require creativity or novel contribution to attract database protection only a substantial investment in obtaining, verifying, or presenting database contents.[248]

4) The Directive offers no guidelines to determine the level of investment required to justify the property right in the database or to extend the duration of an existing right.[249]

5) The Directive's database right potentially erodes the idea/expression dichotomy from copyright law.[250]

6) The Directive's potentially unlimited term of protection, coupled with the strong proprietary nature of the protection and the lack of significant fair use exceptions to the property right,[251] dramatically

---

246. E.U. Directive, *supra* note 27, art. 7; Reichman & Samuelson, *supra* note 9, at 84-85.

247. E.U. Directive, *supra* note 27, art. 10; LLOYD, *supra* note 97, at 189; Reichman & Samuelson, *supra* note 9, at 84-85.

248. E.U. Directive, *supra* note 27, art. 7; Reichman & Samuelson, *supra* note 9, at 84-85.

249. Reichman & Samuelson, *supra* note 9, at 84-86.

250. *Id.* at 87-90.

251. Article 9 of the E.U. Directive provides some fair use exceptions to the database right relating to: (a) private use of the contents of a non-electronic database, (b) use for illustration for teaching or scientific research as long as the source is indicated and there is a non-commercial purpose, and (c) use for public security or an administrative or judicial procedure. E.U. Directive, *supra* note 27, at art. 9. However, the Article is not mandatory; that is, E.U. Member States have the option whether or not to enact any of these exceptions into domestic law. This Article differs from the original draft WIPO Treaty on databases (which was never brought into force). Article 5(1) of the Draft Treaty provides that: "Contracting Parties may, in their national legislation, provide exceptions to or limitations of the rights provided in this Treaty in certain special cases that do not conflict with the normal exploitation of the database and do not unreasonably prejudice the legitimate interests of the rightholder." WIPO, Draft Treaty, *supra* note 86, at art. 5(1). However, it should be noted that the Treaty in general takes a different approach than the E.U. Directive. It does not expressly grant a property right in a database. Rather, Article 3(1) of the Draft Treaty gives the maker of a database the right to "authorize or prohibit the extraction or utilization of its contents," apparently leaving it to Contracting States to decide how to achieve this in practice. *Id.* at art. 3(1). Article 4(2) of the Draft Treaty contemplates that rights granted under the treaty shall be freely transferable and this may, in fact, connote an intention to create a property right in a

erodes the public domain and potentially over-commidifies information products.[252]

7) The final Directive's deletion of the compulsory licensing provision for sole source providers of information creates nearly insurmountable barriers to entry for potential second-comers into information markets and secondary markets.[253] The compulsory licensing provision had been the one aspect of government oversight contemplated in the E.U. database debate.

Looking at the way in which the E.U. Directive has been transposed into national law in various E.U. Member States, most of these concerns appear justified. For example, provisions in the United Kingdom's 1997 domestic legislative enactment—the Copyright and Rights in Databases Regulations 1997 ("CRDR")—raise precisely these concerns.[254]

The CRDR defines a database broadly to include both paper-based and electronic databases.[255] A "database right" is created in a database if there has been a "substantial investment in obtaining, verifying or presenting the contents of a database."[256] Thus, in keeping with the aims of the legislation, there is no reference to creativity or innovation other than that required in section 3A(2) of the CDPA in relation to copyright protection for a database.

A person infringes a database right if that person extracts[257] or reutilizes[258] all or a substantial part[259] of the contents of a database without

---

database, as arguably might the fact that the treaty also contemplates (in Article 8) that a specific term of protection would be established in years in relation to the rights granted to a database maker. *Id.* at art. 4(2). The grant of rights for a particular period of time would seem to be in keeping with notions of proprietary monopolies limited in time as is the case with copyright and patent.

252. Reichman & Samuelson, *supra* note 9, at 87-90.

253. *Id*. at 86.

254. Copyright and Rights in Databases Regulations, (1997) SI 1997/3032 [hereinafter CRDR].

255. The definition of "database" for these purposes is found in the CDPA. *See* CDPA, *supra* note 80, § 3A(1); LLOYD, *supra* note 97, at 177-78.

256. CRDR, *supra* at note 254, at R. 13(1).

257. "Extraction" means the permanent or temporary transfer of database contents in any form to another medium by any means. *Id*. at R. 12(1).

258. "Reutilization" means making the database contents available to the public by any means. *Id.*

259. As contemplated in the E.U. Directive, a "substantial" part of a database's contents is defined in both quantitative and qualitative terms. *Id.*

the consent of the owner of the database right.[260] In this context, the repeated and systematic extraction or reutilization of insubstantial parts of a database's contents may amount to the extraction or reutilization of a substantial part of those contents.[261]

CDPA appears to give strong proprietary rights to database makers The infringement provisions are broad, and the fifteen-year protection term[262] is extendable upon "substantial" changes to the contents of the database, including changes from successive additions, deletions, or alterations.[263] These provisions exemplify the operation of some of the concerns voiced by Professor Reichman, Professor Samuelson, and other commentators.[264]

The English database right is limited by exceptions allowing a lawful user to use a database. The CDPA defines "lawful user," rather unhelpfully, in Rule 12(1) as a person who has a right to use the database, whether under a license to do any of the acts restricted by the database right or otherwise. For example, a lawful user of a database that has been made available to the public is entitled to extract or reutilize *insubstantial* parts of the database contents for any purpose.[265] Additionally, a lawful user may extract a *substantial* part of such a database as an illustration for teaching or research but *not for any commercial purpose* provided that the source is indicated.[266]

This example again supports avoiding the copyright model altogether when drafting *sui generis* database protection. That is, it is important to avoid creating relatively broad rights and then struggling to ascertain the permitted fair use exceptions to those rights. Again, it is easier to clearly and tightly restrict the creation of the rights in the first place.

One way to achieve this would be to limit the definition of database for the purpose of any *sui generis* legislation and tailor relevant rights and liabilities to reasonable commercial activities concerning the database as so defined. Government scrutiny and supervision in the creation and commercial exploitation of the database in clearly identified markets may also assist here. Such an approach would take pressure off the legislators

---

260. *Id*. at R. 16(1).
261. *Id*. at R. 16(2).
262. *Id*. at R. 17(1)-17(2).
263. *Id*. at R. 17(3).
264. *See*, *e.g.*, DAVID, *supra* note 69, at 22-23; Austin, *supra* note 52; Brown, Bryan, & Conley, *supra* note 40; Davison, *supra* note 130, at 283-84.
265. CRDR, *supra* at note 254, R. 19(1).
266. *Id*. at R. 20(1).

to delineate workable fair use provisions, a task which has proven difficult in both the copyright and database right context.[267]

Many of these comments apply equally to a tort/misappropriation model of database protection legislation. Any model may attract such criticism where the rights created in the first place are broad because the definition of database is too broad or vague. This may be the case even if the actual database rights granted under a tort/misappropriation model are weaker rights than those granted under a pure proprietary model.

Thus, a tort/misappropriation model of database protection that has even the indirect effect of creating implied proprietary rights in a broad array of databases (including educational, scientific, personal, or paper-based databases) may well experience similar difficulties with delineating permitted fair use exceptions as an expressly proprietary model of database protection. This is arguably the case with the Consumer and Investor Access Bill even though its prohibitions on database use are significantly more limited than those in the E.U. Directive.

Returning to the "lawful use" exceptions in English database law: there is no definition in either the CDPA or CRDR of "commercial purpose" relating to the "lawful use" provisions. Thus, difficult interpretative questions may arise as to whether particular teaching and research activities involving databases are permissible.[268] A commercial purpose may be unclear in an era in which institutions such as universities have the potential to commercialize to an extent previously unpracticed research products and teaching materials in competition with other institutions.[269]

In any event, it also seems possible that the CRDR provisions allowing extraction of database contents as illustration for teaching or research and not for any commercial purpose may have "illustration" interpreted narrowly. It is likely difficult to use database contents for illustration without also using them for broader research and educational purposes that led to the need for the illustration in the first place.[270]

5. Critiquing the E.U. Approach

In summary, a brief look at the United Kingdom's transposition of the E.U. Directive into domestic law raises concerns about the creation of

---

267. DAVID, *supra* note 69, at 6; LEAFFER, *supra* note 81, at 428.

268. NAT'L RESEARCH COUNCIL, *supra* note 55, at ch. 3.

269. Jacqueline Lipton, *The E.U. Database Right and University Teaching Materials*, 1 J. INFO., L. & TECH (2002), available at http://elj.warwick.ac.uk/jilt/02-1/lipton.html (last visited June 18, 2002) [hereinafter Lipton, *E.U. Database Right*].

270. DAVID, *supra* note 69, at 23; Reichman & Samuelson, *supra* note 9, at 92-93.

broad database rights with vague and narrow exceptions. The structural reason for this is the broad definition of database, leading to a potentially broad array of prohibited conduct, which is only tempered by vague "lawful use" exceptions.

Sui generis database protection law throughout the European Union is still in its nascent stages and time will tell how serious these problems will ultimately become in practice.[271] Therefore, it may not be too late for some legislative changes to be made in the European Union if it can be demonstrated that a more desirable model of database protection legislation is possible, particularly if the United States subscribes to such a model.[272]

Many of the commentators who have criticized the operation of the new database rules throughout the European Union hail from the United States. One reason for this is that recent moves by E.U. Member States to enact database legislation raise an imperative for the U.S. Congress to take similar action. If Congress fails to do so, businesses may perceive greater protection for their databases in Europe and may then set up operations in E.U. Member States rather than in the United States.[273] Indeed, given the perceived problems with current E.U. measures, many American commentators hope that Congress does not "make the same mistakes" as the European Union.[274]

IV. NEW DIRECTIONS IN DATABASE PROTECTION

The best model for database protection legislation may yet emerge from the national or international debates. The current debate has been too closely tied to copyright models simply because the need for database protection legislation has been based on the perceived failings of copyright law to adequately protect digital database contents. Models based too closely on the law of trade secrets and unfair competition will also likely be ineffective for the same reasons previously discussed.

Future discussions should take a new turn altogether, leaving the inadequacies of copyright law aside and focusing purely on the realistic

---

271. Early case law and commentary suggests that some difficult interpretative questions about the scope of the legislation amongst E.U. Member States are already emerging in practice: British Horseracing Bd. Ltd. v. William Hill Org. Ltd., [2001] R.P.C. 31, [2001] 2 C.M.L.R. 12 (Eng. Ch. Pat. Ct.), *available at* 2001 WL 98034; Colston, *supra* note 12.

272. Colston, *supra* note 12, §§ 5, 5.3.

273. Boyarski, *supra* note 104, at 907-08

274. *Id.*; Reichman & Samuelson, *supra* note 9, at 95.

commercial needs of database producers and on the needs of society, domestically and internationally.

We need a completely new approach that looks to the operation of trademark, and to some extent, patent law as models involving the commercialization of information property rights, accompanied by significant government oversight. As argued in the next section, laws creating commercially exploitable rights over non-creative information products require government regulation and monitoring because of the dangers inherent in leaving it to the market to monitor the exploitation of often mundane information and ideas whose value lie not in their creativity, but in their comprehensive collation.

A. Elements for a Comprehensive Database Protection Law

American businesses may currently be disadvantaged vis-à-vis their E.U. counterparts because they are less able to protect database contents and because the E.U. Directive does not provide reciprocal protection to the United States.[275] Today, E.U. businesses can arguably extract an American database's contents for reutilization in their own business and obtain a database right for this copied product while facing limited or no legal redress from the original American database maker.[276] Given the absence of any empirical evidence, it is unclear whether this is currently a problem. Furthermore, American database producers can use restrictive contracts and technological measures to protect database contents from much unauthorized activity.

If the U.S. Congress, however, fails to act on database protection, it may eventually be forced to do so as part of a global harmonization initiative. By failing to take prompt action, the United States might be relegated to following the lead of other countries, regardless of how irrelevant or unattractive those laws may be to the American businesses.[277]

The model I propose for the United States could ultimately be adapted internationally. This model focuses on the registration and commercial exploitation of databases, and overcomes some of the weaknesses inherent in current approaches. It uses mechanisms borrowed from trademark and patent law to create property rights in data compilations in order to *monitor*, *control*, and *limit* the exercise of the rights. Furthermore, it

---

275. *See* E.U. Directive, *supra* note 27, art. 11; Boyarski, *supra* note 104, at 907-08.

276. In fairness, it should be noted that several commentators have suggested that the argument in favor of legislation in the United States based on the fact that American database producers will now be disadvantaged vis-à-vis the European Union is not very convincing in practice. *See* NAT'L RESEARCH COUNCIL, *supra* note 55, at ch. 3.

277. *See* Wolken, *supra* note 67, at 1305.

incorporates some government oversight of the database rights and their commercial exploitation in order to provide significant value to private and public interests alike. Government oversight is not a novel approach to the creation and commercial exploitation of valuable information property rights. Such oversight is already found in trademark law and, to some extent, patent law.[278]

The following comments offer suggestions to shift the debate away from a focus on copyright law and the perceived divide between the property and tort/misappropriation approachs.

Reforming database protection law raises closely interrelated issues: (a) the definition of database; (b) the rights that may be given to database producers; (c) necessary exceptions to those rights, including fair use provisions and, more importantly, compulsory licensing; (d) registration of interests in databases; (e) investigation of business plans showing intention to exploit a database in one or more commercial markets; (f) dispute resolution mechanisms. Obviously, government monitoring could be required for many functions such as compulsory licensing, administrative orders releasing certain information to the public or to private individuals, examination of business plans prior to registration, and some dispute resolution.

It should be possible to draft a new law that clearly confines itself to protecting the contents of only commercial databases against unauthorized access, duplication, use, or distribution.[279] To do so, the definition of a commercial database should focus on commercial exploitation in identified markets and exclude certain non-commercial databases. The law should tightly control and limit prohibited activities to the commercial context. The law should only be broad enough to protect those actually investing time and money into a database they intend to commercialize, enabling them to reap the rewards of their entrepreneurial activities.

We should move past debating whether legislatures should create property or quasi-property rights in new intangible information products such as databases. Rather, we must accept that *any* legislative attempt to protect rights in such products will either expressly or by implication

---

278. Trademark and patent systems the world over require some level of government examination prior to registration of a relevant right. The American trademark system also requires various affidavits to be filed relating to good faith use of the trademark in question.

279. The query needs to be raised here, and is taken up below, whether *duplication* should be prohibited under any new law. This may make the model seem too much like a new version of copyright law and, in any event, may go well beyond the realistic commercial needs of database producers.

create a new form of legal property. Balancing those rights against competing public and private interests should be the core debate.

The thoughtful and careful creation of new property rights can help find and maintain an appropriate balance among the interests of creators, users, and society. Property rights serve as a useful mechanism to prevent undesirable incursions into the public domain of information and ideas. They are only dangerous and undesirable when created without sufficient thought to the necessary needs of those lobbying for them and the obligations imposed on those asserting such rights. These obligations may involve submission to government examination of applications for the property right, compulsory licensing, and other limitations on the right's commercial exploitation. Governmental control and monitoring of information property rights have proven successful in patent[280] and trademark law.[281] Compulsory licensing has also been used for some classes of musical works in the United States.[282]

Database protection law should provide a safe environment that encourages people to produce and commercially exploit valuable databases without creating unfair monopolies over mundane information. To achieve this, new law must address which databases it will protect; how it will create, qualify, and administer such protection; what is permitted and prohibited; and how long protection will last.

B. Criteria for Protection

A database may have multiple purposes, one of which may be commercial. For example, a database may be created in an educational or scientific setting with or without the intent to commercialize it. If created

---

280. Patent law has traditionally required inventors to submit to an examination of their claimed invention and to have their patented invention published on the relevant patent register(s) for ultimate consumption in the public domain when the patent term expires. Additionally, compulsory licensing of certain patents has been utilized in some jurisdictions such as the United Kingdom. *See* Patent Act, 1977, § 48 (Eng.). And is required in the United States by TRIPs with respect to certain pharmaceuticals. *See* Dora Kripapuri, *Reasoned Compulsory Licensing: Applying U.S. Antitrust's "Rule of Reason" to TRIP's Compulsory Licensing Provision*, 36 NEW ENG. L. REV. 669, 681-83 (2002); Patrick Marc, *Compulsory Licensing and the South African Medicine Act of 1997: Violation or Compliance of the Trade Related Aspects of Intellectual Property Rights Agreement?*, 21 N.Y.L. SCH. J. INT'L & COMP. L. 109, 115-16 (2001); Joseph A. Yosick, *Compulsory Patent Licensing For Efficient Use of Inventions*, 2001 U. ILL. L. REV. 1275, 1278-79, 1282 (2001).

281. Trademark law requires public registration of a market in respect of one or more identified markets.

282. 17 U.S.C. § 115 (2000) (providing for compulsory licensing for non-dramatic musical works).

with the intent to commercialize, as many scientific and educational databases currently are, then the database should be protected by the law. If not, then it should not be protected.

The database protection model described here is intended to promote commerce and to balance this aim against the need to protect a vibrant public domain of information and ideas. Where a database is created without any commercial intent, it should be preserved as a public domain resource, particularly if it is created with the support of government funding.[283] Where there is either a wholly or partly commercial purpose, the legislative scheme should assist with the commercialization objectives while preventing unfair commercial monopolies of information and ideas.

The law should not require that commercialization be the sole purpose for which a database has been created in order to attain protection. However, it should at least provide that a bona fide intent to commercialize a database be a significant purpose behind its creation. In identifying a bona fide intent to commercialize a database, the law should recognize that not all database producers necessarily plan to commercially exploit their databases immediately on creation. This is a difficult issue, because it runs contrary to law's goals to allow anyone to propertize information without actually commercializing it or imminently planning to commercialize it. Possibly, producers that create a database for exploitation at some future time should rely on trade secrecy and contractual non-disclosure agreements until they decide either to release the database into the public domain or to register and commercialize it as a protected database.

Legislators would also have to consider a compulsory licensing scheme for registered databases particularly for sole source information providers. Any new law should establish an administrative body to decide issues of compulsory licensing and to apply any legislative exceptions to database protection based on public interest considerations. The body should be empowered to order the release of information into the public domain or into the hands of private individuals such as scientists and educators.

Compulsory licensing is a difficult and contentious issue, particularly when people believe the government should not make decisions about commercial exploitation and access to valuable information. However, there may be no viable alternative. There is also a clear distrust of the market in this area, and significant concern about the commodification of

283. As noted above, open source licensing may be one way of ensuring that information released into the public domain remains in the public domain.

information and ideas generally by market players.[284] The same may be said of empowering an administrative body with the authority to make orders that certain information be released into the public domain or into the hands of named individuals for public interest purposes.

To inspire public trust of the administrative body and its procedures, the law should require the authority (a) to maintain some transparency in its decision-making functions; (b) to keep public records of its decisions; and (c) to hear from parties concerned with a compulsory license or a public information disclosure. Additionally, to achieve a breadth of expertise, the authority should include representatives nominated or appointed by different sectors of society, science, and commerce.

C. The Stand-Alone Database Register

Establishing a register of database rights[285] to show ownership of a database would further promote the purpose of the law. As in trademark law, such a register would allow database owners to exploit their databases in commercial markets with at least some government examination and oversight. By recording the database producers' groundwork in compiling their products and tracking original data sources, the register serves as a central source for adjudicating database rights. Such registration and administration should be completely separate from existing intellectual property regimes such as the copyright, patent, and trademark registers; it should be a *sui generis* body specialized in overseeing database rights.

Establishing a stand-alone database register would help solve the problem of ascertaining if and at what time a database maker intended to commercialize its database. Surely, if a producer has put effort into the development of a database with the intent to profit, it is no great impediment to require the registration of the database rights.

The law might also require the database maker to specify in the registrer the markets in which it intends to commercialize the database.[286]

---

284. Jacqueline Lipton, *Information Wants to be Property: Legal Commodification of E-Commerce Assets*, 16 INT. REV. L COMP. & TECH 53 (2002) (discussing moves in a number of jurisdictions towards the increasing propertization of information products) [hereinafter Lipton, *Information Wants*]; Reichman & Samuelson, *supra* note 9, at 52-53 (discussing the concern about creating powerful property rights in databases in the United States; Therien, *supra* note 36, at 1029 (discussing concerns that the DMCA will over-propertize digital information if courts do not take an adequate stance on protecting "fair uses").

285. Wolken, *supra* note 67, at 1296.

286. The register here might be supplemented with an "intent to commercialize" procedure for databases, not unlike the "intent to use" procedures found in the law of

As with trademark law, the database law would not protect uses the maker fails to specify in the register.[287] This specificity could safeguard the interests of those who want to use the information in secondary markets not in direct competition with the original database producer.

The legislation provisions setting out prohibited conduct could be expressly linked to the markets identified by the database right owner in the register. For example, the provisions could prohibit use of all or a substantial part of the database contents in any market specified in the register. If the legislation followed this approach, provisions may be necessary to ensure that a registrant does indeed use the database in the specified markets within a reasonable period after registration. Failure to do so might result in the loss of registration for that market.

Alternatively, infringement could be limited to uses of all or a substantial part of a registered database's contents *in competition with* the registrant in any market specified in the register. The inclusion of the "in competition with" requirement could prevent database producers from attempting to stifle activity in a market that it has not yet entered in order to reserve the market for itself. However, even this approach would benefit from also requiring the database right owner to enter a specified market within a particular time after registration or risk losing registration for that market.[288]

---

registered trademarks. *See* 15 U.S.C. § 1051(b) (2000); BOUCHOUX, *supra* note 74, at 65-66.

287. There is perhaps an imperfect parallel here with the way trademark registration systems tend to require an applicant for registration to identify the goods and services for which the mark is to be used. Protection under the relevant legislation will be granted for those goods and services. BOUCHOUX, *supra* note 74, at 47-52. In the database case, it would not be goods and services that the applicant was required to note on the application for registration, but markets in which the applicant intended to exploit the database. In this regard, it may help if a domestic, or even international, classification system for relevant markets could be established, not unlike the WIPO Classification System for goods and services in trademark law. *See* WIPO, LIST OF CLASSES OF GOODS AND SERVICES ESTABLISHED BY THE NICE AGREEMENT CONCERNING THE INTERNATIONAL CLASSIFICATION OF GOODS AND SERVICES FOR THE PURPOSES OF THE REGISTRATION OF MARKS, (on file with author), *available at* http://wipo.org/madrid/en/index.html (last visited June 19, 2002).

288. This could be tempered by provisions that a delayed entry into a market might not result in loss of registration for that market if the database right owner can give a reasonable explanation to the administrative authority explaining the delay and if there would be no discernable negative effects on the market as a result of the delay coupled with a renewed grace period.

D. Investigation and Validation

To ensure the integrity of the register, the model would also require an officer from the administering body to investigate and validate an application prior to registration. This is somewhat similar to patent law, although the process for database rights would involve different steps: (a) investigating other database rights registered in the same or similar markets to those claimed by the applicant, (b) ensuring that the database in question is at least almost ready for commercialization, and (c) checking that the applicant has *bona fide* plans to commercialize the database in the markets identified in the application.

When investigating other registered rights, the aim would be to secure rights in a database version against unauthorized reuse of its contents in that market, not to reserve all rights to use a database in a market to the first registrant. Thus, more than one market player could register a database right in the same market provided that no unauthorized extraction of contents had taken place in that market. If a second database producer has compiled a similar database to the original registrant by going back to the original information sources, the second producer should be equally entitled to claim and register a database right in the same market.

It could be a condition of registration that a database producer take all reasonable steps to identify its own database contents through the use of available technology like watermarks. With the use of watermark technology to track the original sources of data, database-producers should be able to provide evidence to the registration authority of unauthorized extraction or reuse. This could help resolve later disputes over unauthorized extraction or reuse when the competing databases use similar material in the same market.[289]

For example, Company A sets up an online travel agency with a database of airfares obtained by negotiating directly with airlines and then Company B does precisely the same thing. Both companies should be able to claim and register a database right in the same market, which differs from trademark law. In cases where one database producer is claiming unauthorized extraction or reuse of contents by another database producer in the same market, the register would evidence a clear record of compilation groundwork and the original sources of data, supplemented by

289. The database administration authority might also take on a "public education" function to advise people on how best to utilize available technology to protect databases. This is another useful function that government authority and oversight can add to its role in creating and protecting reasonable intangible property rights. *See* Lipton, *Commercial Information*, *supra* note 54, at 26-28.

evidence of digital watermarking.[290] The register should limit the scope of property rights in databases rather than create potential monopolies in database markets.

The second stage of the investigative process would ensure that applicants do not attempt to register ideas for databases in which they have not yet invested any time, effort, or capital. To satisfy the commercial intent requirement, the new rules should require applicants to show concrete business plans for the database in a particular market. Those who have not yet developed a database to the commercialization stage would likely opt to maintain trade secrecy until they are ready to register and commercialize the database. For those who have developed a database to the commercialization stage, it is not particularly onerous to require the disclosure of a business plan, particularly if such plans were kept confidential by the administrative body.

The law should include a provision that failure to commercialize a registered database within a certain period after registration would result in the loss of registration for the specified markets. This would encourage database producers to plan carefully for commercialization and only to register in markets in which they realistically intend to pursue commercial activities. This, in turn, would help prevent the chilling effect caused by a database producer registering in markets that it has no *bona fide* intention of entering. The timely commercialization provision could be supplemented by requiring affidavits of "continuing use" for database rights, not unlike the "affidavits of use" required in registered trademark law.[291] This requirement would ensure the database's continued use, weed out abandoned and frivolous claims from the register, and quell the chilling effect described above.

E. Duration of Database Rights

The next step is to address the appropriate *duration* for a database property right. The alternatives are (1) a fixed term of years[292] or (2) a duration based on the information's value and the effort put into compiling

290. Hector MacQueen, *Copyright and the Internet*, *in* LILIAN EDWARDS & CHARLOTTE WAELDE, LAW AND THE INTERNET: A FRAMEWORK FOR ELECTRONIC COMMERCE 202 (2000).

291. For trademarks, failure to submit the affidavit within the appropriate timeframe leads to loss of registration of the mark. 15 U.S.C. § 1058(a)-(b) (2000); BOUCHOUX, *supra* note 74, at 72.

292. This tends to be associated with copyright/property models of database protection.

the information.[293] A fixed term of years is easier to draft, particularly if duration is measured from the date of registration. Under this scenario, the term should be significantly less than the E.U. Directive's extendable fifteen-year term.[294] Three or four years of initial protection should be sufficient to give a database maker a head start over competitors.[295]

Even in the case of a continually updated electronic database, the term of protection should be limited to the term of the initial database because that protection is sufficient to give the database producer its head start. A database producer should not be able to claim ongoing proprietary rights in a database simply for keeping the database up-to-date.[296] True, a competitor could wait until the database loses its protection and then copy both the original database and any updates. To prevent this, however, legislation could include provisions limiting what competitors can do with existing databases.

However, as a matter of public policy, a competitor *should* be able to copy a database and all updates after the original database producer has had its head start. In this case, the competitor may have to add some value to its copied database in order to draw customers away from the original database maker.

The second approach to duration of protection, which emphasizes the prevention of unfair competition by another commercial entity, may produce fairer results.[297] This approach bases duration on the value of the database's information or the value of the effort put into compiling the information.

---

293. This tends to be associated with tort/misappropriation models of database protection.

294. *See* E.U. Directive, *supra* note 27, at art. 10.

295. On appropriate fixed terms of protection for *sui generis* database rights, see Austin, *supra* note 52, ¶ 86. *See also* Wolken, *supra* note 67, at 1301.

296. This is currently the situation in the E.U. where continually updating a database will effectively result in indefinite proprietary protection. The E.U. Directive provides that

> [a]ny substantial change, evaluated qualitatively or quantitatively, to the contents of a database, including any substantial change resulting from the accumulation of successive additions, deletions or alterations, which would result in the database being considered to be a substantial new investment, evaluated qualitatively or quantitatively, shall qualify the database resulting from that investment for its own term of protection.

E.U. Directive, *supra* note 27, at art. 10(3).

297. *See, e.g.*, U.S. COPYRIGHT OFF., *supra* note 100; Reichman & Samuelson, *supra* note 9, at 139-44.

Such an approach also has serious drawbacks such as establishing who should determine the duration of protection and on what evidence. Presumably, a newly established administrative body would decide the duration for any given case. This body would gradually develop expertise in relevant market issues, including the fair duration for a database right. This administrative body should include experts with detailed knowledge of information markets from commerce, science, and education.

We must note that we are only considering how long one market player can assert proprietary rights against others. We are not necessarily balancing private and public interests. The database protection scheme advocated here would grant proprietary protection only to commercial databases. The key issue with duration is not how long a market player can own information and prevent public access to it, but rather how long a market player can assert a right to commercialize a database against a competitor.

Other aspects of the legislation would protect public interests by allowing the administrative body to order the release of information to the public domain or to one or more nominated individuals. Although the tasks are difficult, an administrative body with experts in relevant fields capable of examining expert evidence would tend to create better results than those created purely by market forces.

Another potential downside with this approach would be the difficulty maintaining a usable database register if databases attracted different terms of protection in different markets. Thus, a straight proprietary-based model for term of protection may be preferable, particularly if it was limited to an initial term of three or four years. Perhaps, this term could be extended on application to the registering authority with evidence to showing, for example, that unfair competition would occur in a market if the protection were not temporarily extended.

In this way, a limited proprietary model could be augmented by aspects of a tort/misappropriation model relating to the prevention of unfair competition or unjust enrichment. The possibility of drafting a law on this basis again shows that new *sui generis* database law need not be a choice between a proprietary and a tort/misappropriation model. Elements of each may be useful, and the two approaches may be merged if the focus is placed on developing appropriate foundations for the law from first principles.

F. Permitted and Prohibited Activities in Relation to Database Rights

What should a database law permit and prohibit in order to achieve its purpose? Rationally self-interested database producers will want to allow access of database contents to authorized persons, prohibit others from access, and prevent unauthorized copying or distribution.[298] The prohibitions set out by law should be limited to preventing *competing commercial uses* of a database in the markets for which it has been registered. This focus on competing commercial uses draws partly on principles of trademark law and partly on the approach in the Consumer and Investor Access Bill.

In this respect, Professor Conley goes too far by identifying the copying of database contents per se without a concurrent use or distribution of those contents in commerce as an activity that a database producer would seek to prohibit. Though Professor Conley may be correct in proposing that a rationally self-interested database producer would want to prohibit copying per se, this concern likely owes more to the influence of copyright law on database protection initiatives than to any realistic commercial concerns of database producers.

Even a model based on limiting the definition of a database to the commercial field would likely require some public policy permitted uses enhanced by a compulsory licensing program.[299] However, focusing on commerce and registration of commercial interests should make it easier to carve out these exceptions when compared with the current models of database protection legislation.

To accommodate such permitted uses, the law should ensure that permited activities cannot be effectively precluded by contract or technological protection measures. The ability of the administrative body to order the release of certain information or to make a compulsory licensing order could minimize problems with contractual or technological protection measures.[300]

G. The Administrative Body

For the law to work, it must establish an expert administrative body to oversee the registration of database rights, the compulsory licensing of

---

298. Brown, Bryan, & Conley, *supra* note 40, ¶ 34.

299. *See* Austin, *supra* note 52, ¶ 87.

300. Cohen, *supra* note 65, 607-09 (noting that public policy considerations may be used to support legislation that overrides contract and technological protection measures in relation to digital information products).

database contents,[301] and the release of database contents into the public domain. This body would require experts from database-utilizing sectors in science, technology, education, and commerce.

An administrative body would have the advantage of a clear and centralized focus on database issues, allowing it to develop expertise in this area. This centralizing function should promote consistency and efficiency when deciding database issues.

For example, the centralization created by the Uniform Dispute Resolution Policy ("UDRP")[302] for Internet domain name disputes has streamlined disputes that were tried in a variety of national fora, applied different laws, and often created inconsistent results.[303]

The domain name dispute resolution procedure is not a perfect analogy to the database scheme suggested here. The UDRP is international in scope and administered by private bodies such as the Internet Corporation for Assigned Names and Numbers ("ICANN"), acting through intentional agents such as WIPO. Furthermore, the UDRP is limited to the resolution of disputes and does not deal with issues such as whether a domain name can be registered in the first place.[304] However, the UDRP does illustrate the potential efficiency benefits of centralizing controversial issues relating to a particular class of digital information assets in a body that can gradually develop an expertise in the area.[305]

---

301. A detailed discussion of the precise situations in which compulsory licensing might be allowed/required is beyond the scope of this preliminary discussion into changing the basic direction of the database protection debate. However, it does seem that whatever model of database protection legislation is ultimately brought into play (if any), there needs to be some possibility of compulsory licensing certainly in the case of sole source information providers and arguably in some other situations where the database protection legislation is causing practical results that are undesirable as a matter of public policy. One example might be in the difficult area of scientific and educational databases that often have competing commercial and non-commercial applications. The availability of an expert administrative body that might decide questions relating to the possibility of compulsory licensing in such cases could be a valuable addition to/improvement on some of the previously discussed models for database protection legislation.

302. INTERNET CORP. FOR ASSIGNED NAMES & NUMBERS, UNIFORM DISPUTE RESOLUTION POLICY, *available at* http://www.icann.org/dndr/udrp/policy.htm (last visited May 11, 2003) [hereinafter UDRP].

303. *See* LEMLEY ET AL., *supra* note 13, at 676-82 (describing the operation of the UDRP).

304. UDRP, *supra* note 302, cl. 3.

305. In actual fact, the dispute resolution functions under the UDRP are currently concentrated in three distinct bodies authorized by ICANN to hear domain name

In fact, an administrative entity specializing in database issues could also hear, as an alternative to litigation, disputes involving rights in databases. This would have the advantages usually associated with alternative forms of dispute resolution such as reduced cost, the expertise of people hearing the dispute, and perhaps confidentiality and informality.[306] Presumably, as with the UDRP, such a system would not be able to oust the court's jurisdiction entirely.[307] However, some disputes could be kept out of court if those with registered databases were required to submit to an administrative proceeding before starting litigation on a database dispute.

Collecting database disputes together in one place, at least initially, could also minimize inconsistent interpretation of the legislation by different courts. This would encourage judges to examine the reasoning of the administrative body before making judicial determinations on the same or similar fact situations. Thus, in a database dispute resolution system along the lines suggested here, the administrative determinations should be published to aid judges, assuming, of course, that the administrative proceedings in question are not confidential in nature. The initial debates about the establishing the framework for the administrative system would determine whether such proceedings would be confidential.

H. Unregistered Databases

As with trademark law, a new database law should specify the legal position on non-registered databases used in commerce. This could follow the trademark model and permit developers of unregistered databases to protect them under other laws (such as contract, copyright, or trade secret) where applicable, but deny protection under the *sui generis* law.[308]

It may also be a good idea for the legislation to require or advise owners of registered database rights to include registration details on their databases, giving others notice of the existence of the rights.[309] Failure to

---

disputes. However, the WIPO arbitration panel does hear the majority of disputes and so is an important centralizing force here.

306. *See, e.g.*, RICHARD GARNETT ET AL., A PRACTICAL GUIDE TO INTERNATIONAL COMMERCIAL ARBITRATION 11-14 (2000).

307. UDRP, *supra* note 302, cl. 4(k) (preserving the parties' rights to litigate a domain name dispute subsequent to the administrative proceeding).

308. An example of such a model can be found in the United Kingdom trademarks legislation. The 1994 Trade Marks Act provides that, although common law (unregistered) marks are not protected under the legislation, nothing in the Act affects law relating to the tort of "passing off" with respect to protecting unregistered trademarks. *See* Trade Marks Act, 1994, § 2(2) (Eng.).

309. Wolken, *supra* note 67, at 1296.

give notice could result in loss of statutory protection for the rights. Again, this places a strong onus on those seeking legal protection to take reasonable steps to protect the intellectual property rights they wish to assert in their work. In this way, the law would provide incentives to registered database holders that incorporate technological protection measures such as digital watermarks into their databases.[310]

I. Benefits of Database Law Reform

Drafting a model database law using the methods discussed above has several advantages over existing legislation. For example, clearly restricting the concept of a protected database to those databases developed for commercial purposes would be beneficial. This will focus the law on realistic *commercial* objectives and will lessen the focus on often-problematic fair use provisions. Furthermore, using a registration system for commercial databases will help to clarify who owns what rights and in what markets. It will create greater clarity and certainty in database proprietorship and in permitted activities in databases.

Another benefit would be the establishment of a specialist administrative body to oversee database registration, commercial disputes, and requests to release database contents. Such an approach would focus and centralize issues relating to databases, taking those issues outside the realm of pure market control. Whatever problems there might be with a centralized administrative body, reliance on pure market forces would not likely achieve better results, particularly in protecting the public domain and individual competing interests in information.

Any new database law should not derogate from pre-existing intellectual property rights that may apply to a database, such as copyright in the selection or arrangement of contents of a particular database.[311] The rights embodied in the new law should be distinct from existing intellectual property rights and should be able to co-exist without interfering with the balance of other intellectual property laws.[312]

---

310. *See* MacQueen, *supra* note 290.

311. CDPA, *supra* note 80, § 3A(2); Feist Publ'ns v. Rural Tel. Serv. Co., 499 U.S. 340, 340 (1991).

312. It has been clearly accepted in the past that different intellectual property rights can co-exist in the same item at the same time; they simply protect different attributes of the item in question. This model has been adopted in the United Kingdom with respect to rights in databases as a result of the E.U. Directive. The English legislation specifically contemplates that a database right and a copyright may co-exist in the same database at the same time and will simply protect different aspects of the database. CRDR, *supra* at note 254, R. 13(2).

V. THE INTERNATIONAL DIMENSION

A. The International Picture on Database Protection

Whether or not the proposed solution would be attractive to the United States, efficient database protection legislation faces a greater problem: globalization. Now that many electronic databases are easily accessible internationally, the U.S. approach to database protection will impact and be affected by the international sphere. The European Union has already enacted database protection legislation that gives broad proprietary protection to database contents but without sufficient public policy exceptions or government oversight.[313] Canada has no database protection legislation but will likely carefully watch the United States and the European Union. As noted above, Australia appears to rely on copyright protection for databases.

If other countries enact database legislation based on the E.U. approach, international harmonization may be achieved. But this could sacrifice significant aspects of the public domain and interfere with the traditional intellectual property framework. On the other hand, if countries like the United States and Canada enact legislation that is out of step with the European Union, the E.U. Member States may have to reconsider their approach to database protection in order to achieve international harmonization.[314]

Perhaps the most important step here is to finish an international treaty on database protection that can be adopted by jurisdictions throughout the world.[315] However, to do so, we must reach consensus on the best way to balance the many rights, liabilities, and exceptions that would form database protection.[316] Thus, these issues should be debated further, particularly between the United States and the European Union, to arrive at a model that achieves an appropriate balance between protecting commercial activities and preserving the public domain. In addition, we must maintain the traditional aims of intellectual property protection; encouraging innovation while protecting the public domain for the advancement of arts and sciences.

Arguably, the European Union has already taken up this debate, but perhaps with insufficient input from the scientific and educational

313. Colston, *supra* note 12, §§ 1, 2.2; Reichman & Samuelson, *supra* note 9, at 55-56; Reichman & Uhlir, *supra* note 29, at 829.

314. Colston, *supra* note 12, §§ 5, 5.2.

315. Davison, *supra* note 130, at 283-84.

316. *See* Reichman & Samuelson, *supra* note 9, at 138.

sectors.[317] The lack of widespread international acclaim for the European Union's current solution further supports the need for revision. Indeed, the operation of the E.U. Directive was supposed to be reviewed in 2002.[318] However, this review has not taken place. There is also supposed to be a forthcoming WIPO report on database protection that takes into account the experiences to date of database protection in the European Union.[319]

B. The Role of International Legislative Cooperation

To achieve international consensus on database protection, states may need to re-draft or amend legislation already in force throughout the European Union in order to attain a degree of international harmonization.[320] This may be politically difficult, but could prevent the currently inadequate database laws from stymieing international commerce.

Many interrelated questions are raised when trying to determine an appropriate level of national and international protection for databases. First, how harmonized must the law be internationally and among jurisdictions in a federal system like the United States, Canada, and Australia?[321] For example, would it cause widespread international conflict for non-E.U. countries to take an approach different than the E.U. Directive but nevertheless to operate alongside its provisions?[322] If other countries favor the model this Article proposes, this integration may prove problematic.

Second, should the form of protection be proprietary or non-proprietary? Does it make a difference? Broad proprietary protections, tempered with detailed exceptions and subject to contractual and technological limitations, may offer no greater protection than narrow quasi-proprietary protections with fewer exceptions.[323] This question may be misplaced. The better focus is on commercial uses of databases

317. *Id.* at 139.

318. Colston, *supra* note 12, §§ 5, 5.2.

319. *Id.* As noted above, the issue of intellectual property protection for non-original databases is back on the agenda for the WIPO committee on Copyright and Related Rights.

320. Colston, *supra* note 12, §§ 5, 5.2.

321. The need to harmonize within a federal jurisdiction is usually not too difficult to satisfy if the measures taken remain in the realm of intellectual property law as this tends to be a matter within federal legislative competence in most federal jurisdictions. Some jurisdictions may need to use federal commerce powers rather than intellectual property powers in this area.

322. Colston, *supra* note 12, § 6.

323. Davison, *supra* note 130, at 283-84.

regardless of whether the legislation adopts proprietary terminology. Registration of database rights for markets could also provide an important (if costly) innovation here. Registration could perhaps work at the international level, either through a series of electronically linked domestic registers or an international register.

Third, is it possible to create appropriate protection for databases without unjustifiably interfering with the traditional societal intellectual property bargain? Any new legislative scheme should recognize the need for a strong and vibrant public domain of information and ideas. Any legislative model that ultimately gains acceptance as the international standard should incorporate some safeguards that protect this public domain. These safeguards may include compulsory licensing or the loss of protection where public policy requires all or part of the information to be released into the public domain. Indeed, governments may need to more actively protect the public domain than they have under previous law.

Fourth, do the legislatures have the competence to enact appropriate legislation? For example, if new database protection does not fall within the U.S. Constitution's Arts and Sciences or Commerce clauses,[324] database protection would have to be attempted as uniform state law, which is contentious and not easy to achieve. Canada and Australia may face similar issues. However, if the federal legislature can be used to support database protection, these issues will not arise. In the United States, opinions divide on whether the Commerce clause can support database protection legislation.[325] Under the Commerce clause, legislation that creates a new intellectual property right that does not promote the progress of the arts and sciences may not be justifiable. Indeed, the Executive Summary of the United States Copyright Office's report on the Legal Protection for Databases in 1997 commented on this problem:

> If database legislation appears to be the equivalent of copyright under another name, but providing protection to uncopyrightable subject matter for unlimited times, the use of a different label and the recitation of a different constitutional basis will not alone be sufficient to save it. To the extent that the legislation promotes different policies from copyright, and does so in a different manner, it is similar to trademark law, and therefore seems likely to survive a constitutional

---

324. Austin, *supra* note 52, ¶ 89; *see also* Benkler, *supra* note 32, at 412-13; Pollack, *supra* note 121.

325. U.S. COPYRIGHT OFF., *supra* note 100, at xviii; Pollack, *supra* note 121.

> challenge. The more the statute differs from copyright, the more likely it is to be constitutional.[326]

This distinction between copyright and trademark law further supports a model for database protection legislation in the United States that moves away from existing copyright law and towards trademark law. Such a scheme would lessen the risk that the law would be found unconstitutional for trying to create a broader version of copyright under a different constitutional head of power.

Fifth, should the law bolster technological protections put into place by database makers to restrict or prevent access to a database? Such bolstering would be similar to what the DMCA did for copyright in the United States.[327] Technological protection and encryption measures will be a useful tool for database producers seeking to prevent unauthorized access to database contents. However, given the criticisms of the DMCA's approach to legally bolstering these protections,[328] perhaps this is not the right approach for *sui generis* database protection legislation.

Sixth, how should any new law deal with inter-jurisdictional problems like having a defendant in another jurisdiction? Could the law deal with situations like the inability to identify the wrongful appropriator of database contents because of anonymous online access? Since notice of a database property right can bind third parties, it would be relatively easy under a proprietary law for a right-holder to identify those wrongfully using its databases in commercial competition, regardless of how that competitor came by those products in the first place.[329] The ability to

---

326. U.S. COPYRIGHT OFF., *supra* note 100, at xviii.

327. Article 10 of the draft WIPO treaty on database protection suggests that database protection legislation should include provisions that make it unlawful to import, manufacture or distribute devices that can defeat such technological protections. *See* WIPO, Draft Treaty, *supra* note 86, art. 10; *see also supra* note 251 and accompanying text. Interestingly, the Draft Treaty remains silent on the question of conduct that actually circumvents a technological protection measure–it concentrates instead on trafficking in devices that could be used to circumvent a technological protection measure. This is a somewhat more limited approach than that taken under the DMCA in relation to the circumvention of technological measures designed to protect copyright works.

328. Benkler, *supra* note 32, at 414-29; Nimmer, *supra* note 33, at 720-26; Samuelson, *supra* note 33, at 537-38.

329. Provided that a third party has notice of the property right, it should be held accountable for its unauthorized conduct in relation to the relevant property, provided that it has no other legal excuse for its conduct, such as a public interest upheld by the relevant administrative body. Notice of a database right is provided by registration and database owners could also be required to display their registered status prominently on their database.

identify such wrong-doers would be increased by using technological measures like digital watermarking to identify the original source of database contents but cross-jurisdictional enforcement may be problematic.

All of these questions are difficult to address in practice. It is unfortunate that the WIPO Database Treaty[330] was not completed in 1996 when the Copyright Treaty[331] and Performances and Phonograms Treaties[332] were completed. Such an agreement would have given guidance for tackling these issues at the international level. The current draft of the treaty is vague. The term of protection to be granted to a database maker is also unclear with a number of options given in the current text.[333] The WIPO Database Treaty requires further debate and redrafting, particularly on the nature of the rights that should be granted to database makers and the necessary exceptions to those rights.

Much work must be done before we can create effective harmonized laws that meet the needs of the global information society. The debate may become clearer if we ignore the question whether databases should be protected as property and instead focus on how to clearly delimit the rights and obligations of those who have developed commerical databases. At the international level, the important issues are (a) how to achieve international consensus and what that consensus should entail; (b) how to determine the level of uniformity needed to support harmonized international database law;[334] and (c) how to effectively translate any

---

330. *See supra* notes 86, 251 and accompanying text.

331. Copyright Treaty, Dec. 23, 1996, World Intellectual Property Organization CRNR/DC/94, *available at* http://www.wipo.org/eng/diplconf/distrib/94dc.htm (last viewed on Aug. 30, 2003).

332. WIPO Performances and Phonograms Treaty, Dec. 23, 1996, World Intellectual Property Organization CRNR/DC/95, *available at* http://www.wipo.org/eng/diplconf/distrib/95dc.htm (last viewed on Aug. 30, 2003).

333. The current draft Article 8 of the treaty suggests the options of a twenty-year *or* a fifteen-year term of protection. *See* WIPO, Basic Proposal for the Substantive Provisions of the Treaty on Intellectual Property in Respect of Databases to be Considered by the Diplomatic Conference (on file with author), *available at* http://www.wipo.org/eng/diplconf/6dc_a08.htm (last visited Sept. 26, 2001). As noted above, even a fifteen-year term of protection is arguably unreasonably long.

334. It should be noted that "harmonization" does not necessarily connote complete uniformity. It is used here to refer to laws that can work together without too many practical conflicts, even if the laws are not framed in precisely the same terms and maybe are not even framed with the exact same theoretical underpinnings in mind. In the database context, the possibility of relatively harmonized, yet not uniform, law is contemplated in Colston, *supra* note 12.

resulting international policies or treaty obligations into harmonized national laws.

We need significant international consensus and guidance on these issues, which could be done through WIPO or UNCITRAL.[335] Thus, a final version of the WIPO treaty on database protection could be a first step in reaching consensus, although this may require some amendment of both the E.U. Directive and the E.U. Member State's national legislation implementing the Directive.

If the United States, either nationally or through WIPO, can present some new models that appear to streamline the process, other jurisdictions may be prepared to adjust their current positions on database protection. A modified E.U. model could even work alongside a somewhat different model in the United States provided that the two approaches maintain compatible administrative and enforcement mechanisms.

C. International Treaty Goals

For an international database protection treaty, issues that warrant consideration include (a) the nature and scope of legal rights for databases with commercial uses; (b) distinguishing between *sui generis* database rights and existing copyright protection for databases and compilations; (c) the nature and scope of exceptions for private, scientific, educational, and research use; and, (d) the an administrative body overseeing registration, compulsory licensing, and dispute resolution.[336]

The original draft WIPO database treaty started to resolve some of these issues on an international level, and the proposed study on the operation of current E.U. law would also help. However, to achieve the level of certainty required to enact meaningful and reasonably harmonized laws at the international level, decision makers must analyze the impacts of *any* database protection law on private, scientific, educational, and research uses.[337] It must also consider whether standard domestic litigation is appropriate for the resolution of domestic and international disputes or whether litigation should be augmented by specially tailored alternative dispute resolution administered by national or international experts.

---

335. UNCITRAL is the core body within the United Nations that deals with international trade issues. It coordinates the drafting of international treaties on matters affecting international trade. More information on UNCITRAL and its activities can be found at http://www.uncitral.org/en-index.htm (last visited June 19, 2002).

336. These might be established at the international level, or possibly through co-operative domestic initiatives.

337. Reichman & Samuelson, *supra* note 9, at 114; Wolken, *supra* note 67, at 1297.

VI. CONCLUSION

In sum, to develop new database protection legislation that protects the public interest and promotes private enterprise in the global digital commons, we must distance the legislation's substantive rights and administration from pre-existing approaches like copyright law. The legislation should focus on database producers' clearly established and realistic commercial needs in order to significanly limit the scope of private database rights. Furthermore, the legislation should create a new specialist administrative body to oversee database rights and resolve issues surrounding the registration of databases, compulsory licensing, database dispute resolution, and the release of database contents into the public domain.

Legislation based on the model outlined in this article would have several advantages. First, database rights could be specifically tailored to the realistic needs of commercial database producers. Second, these needs could be balanced against community concerns over the over-commodification of information. Third, constitutional concerns would arise less often because the law would not focus, like a new form of copyright, on protecting creators of information works but would focus instead on regulating commercial activity.

Establishing a specialized administrative body overseeing database protection would also be helpful. Such a body would ultimately develop centralized expertise on the database industry. And by taking input not only from commercial but scientific, technical, and educational groups, the body could tailor registration and dispute resolution procedures to the realistic needs of different sectors of society.

A successful test of this model in the United States could serve as a template for international approaches to database protection. It may even convince members of the European Union that such a model would work better than the E.U. Directive. If E.U. members are open to making changes in line with such a model, the possibility of international harmonization across jurisdictions would be greatly enhanced. This harmonization would benefit large sectors of industry that increasingly revolve around international information commerce.

Indeed, the global community must rethink approaches to *sui generis* database protection legislation. For example, the property concept itself can be applied to databases in order to strike an appropriate balance between private rights and public interests in databases. The United States has an opportunity to become a global leader in providing effective and efficient solutions to problems involving the legal protection of databases.

Rather than continuing to argue about whether or not we should advocate property in in these valuable information compilations, we should move the debate to another level by advocating the use of property rights to create a balanced system of private rights and public responsibilities.

Looking long-term, any experiment using database property rights to balance different interests may prove a useful template for approaching the regulation of digital information generally. Database rights may be the tip of the iceberg; the next logical development being a body of "information law" or "information property law" that balances competing interests in information in general. Indeed, thinking about new ways of conceptualizing legal property rights in databases may help us to reconceptualize ideas about information property, broadly and globally.

CHEAP DRUGS AT WHAT PRICE TO INNOVATION: DOES THE COMPULSORY LICENSING OF PHARMACEUTICALS HURT INNOVATION?

By Colleen Chien[†]

ABSTRACT

The patent system is built on the premise that patents provide an incentive for innovation by offering a limited monopoly to patentees. The inverse assumption that removing patent protection will hurt innovation has largely prevented the widespread use of compulsory licensing—the practice of allowing third parties to use patented inventions without patentee permission. In this Article, I empirically test this assumption. I compare rates of patenting and other measures of inventive activity before and after six compulsory licenses over drug patents issued in the 1980s and 1990s. As reported below, I observe no uniform decline in innovation by companies affected by compulsory licenses and find very little evidence of a negative impact, which is consistent with earlier empirical work. While anecdotal, these findings suggest that the assertion that licensing categorically harms innovation is probably wrong. Based on the data, I comment on the use of compulsory licensing to reduce the price of AIDS and other drugs for developing countries. I suggest that, based on past experience, compulsory licenses need not result in a decline in innovation and that this policy option for increasing access to medicines deserves greater exploration.

TABLE OF CONTENTS

---

† Associate, Fenwick & West; J.D., University of California at Berkeley School of Law (Boalt Hall), 2002; B.S. & A.B., Stanford University, 1996. I would like to thank Mark Lemley, Fred Abbott, Jenny Lanjouw, Sasha Blaug, and Dirk Calcoen for their helpful comments and support. In addition, I would like to acknowledge Biospace Inc., for generously providing access to its Clinical Competitive Intelligence System clinical trials database. An earlier version of this paper was awarded Grand Prize in the 2002 Third Annual Foley & Lardner Intellectual Property Competition.

I. INTRODUCTION

The international AIDS crisis has posed an acute challenge to the robustness of the patent system. Critics contend that the basic bargain between patentees and the public, namely innovation in exchange for a limited monopoly, is irreparably skewed in favor of drug companies.[1] Defenders of strong patent rights, on the other hand, insist that any weakening of existing protections would undermine the potential for future innovation.[2]

Compulsory licensing, the practice of authorizing a third party to make, use, or sell a patented invention without the patentee's consent,[3] has long provided an antidote to the perceived ills of the patent system.[4] In the context of the AIDS crisis, compulsory licensing offers one way to lower drug prices and increase access to patented medicines in developing countries in which pharmaceuticals have chosen to secure patent protection and the markets supplied by these countries.[5] Under the Agreement on Trade-

1. *See, e.g.*, PASCALE BOULIN ET AL., MÉDECINS SANS FRONTIÈRES, DRUG PATENTS UNDER THE SPOTLIGHT: SHARING PRACTICAL KNOWLEDGE ABOUT PHARMACEUTICAL PATENTS 2 (2003) ("Patents are not god-given rights. They are tools invented to benefit society as a whole, not to line the pockets of a handful of multinational pharmaceutical companies."), *available at* http://www.accessmed-msf.org/documents/patents_2003.pdf (last visited July 19, 2003); Larry Elliot, *Evil Triumphs in a Sick Society*, GUARDIAN, Feb. 12, 2001 (criticizing global patent law for favoring large pharmaceutical companies), *available at* 2001 WL 11917250.

2. *See, e.g.*, Gregory J. Glover, Statement on Behalf of Pharmaceutical Research and Manufacturers of America Before the Federal Trade Commission and the Department of Justice-Antitrust Division, Competition in the Pharmaceutical Marketplace 6 (Mar. 19, 2002) ("[C]ompanies would not be able to invest the huge amount of time and money it takes to discover and develop a new medicine if they did not have a sufficient opportunity to make a sufficient return before generic competitors copy and market the drug at greatly reduced cost."), *available at* http://www.ftc.gov/opp/intellect/020319gregoryjglover.pdf; Richard Tren, *Free Industry, Not the Drugs*, WALL ST. J. EUR., July 11, 2002, at A10.

3. F.M. SCHERER & JAYASHREE WATAL, POST-TRIPS OPTIONS FOR ACCESS TO PATENTED MEDICINES IN DEVELOPING COUNTRIES 13 (Comm'n on Macroeconomics & Health, Working Paper No. WG4:1, 2001), *available at* http://www.cmhealth.org/docs/wg4_paper1.pdf (last visited Aug. 27, 2003).

4. Compulsory licensing was a component of a late nineteenth-century English patent reform bill. *See* Fritz Machlup & Edith Penrose, *The Patent Controversy in the Nineteenth Century*, 10 J. ECON. HIST. 1, 4 (1950). The United States instituted a compulsory licensing provision as early as 1910. Act of June 25, 1910, ch. 423, 36 Stat. 851, 853 (current version at 28 U.S.C. § 1498).

5. Other options include price regulation and improved health infrastructure. *See, e.g.*, Amir Attaran & Lee Gillespie-White, *Do Patents for Antiretroviral Drugs Constrain Access to AIDS Treatment in Africa*, 286 JAMA 1886, 1890 (2001) (noting that numerous drugs are not patented or are off-patent in a number of developing countries, arguing that

Related Aspects of Intellectual Property Rights ("TRIPS"),[6] compulsory licensing is authorized under certain circumstances, such as public health emergencies. However, until recently, few compulsory licenses had been actually issued under TRIPS.[7] One of the most important reasons for this, and the one this Article focuses on, is the perception that compulsory licenses harm the incentive for innovation. In the words of one pharmaceutical executive: "[T]hreatening compulsory licensing . . . will only act as [a] disincentive[] to the development and marketing of new drugs."[8] The twin goals of increasing access to existing medicines and promoting research and development of new medicines have been portrayed as competing with each other.

This Article questions this fundamental assumption. It explores whether past compulsory licenses over drugs have been accompanied by a reduction in innovation, drawing upon past research efforts and the results of an empirical analysis that I performed on six cases of compulsory drug licenses issued in the United States by the Department of Justice ("DOJ") in the 1980s and 1990s. The analysis compares rates of innovation within a therapeutic area, measured by patent counts and other indicia, before and after compulsory licenses were issued.

---

the absence of patent protection neither guarantees nor increases access to drugs, and suggesting that factors such as political will and poverty levels restrict access more than patent protection does); Tobias Buck, *EU Acts to Speed up Flow of Cheap AIDS Drugs*, FIN. TIMES, May 27, 2003, at 6 (describing a proposal by the European Union to cap the price of AIDS, malaria, and tuberculosis drugs sold to developing countries).

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

7. Nonetheless, the threat of compulsory licensing under TRIPS arguably encourages pharmaceutical companies to voluntarily reduce prices. *See* JEROME H. REICHMAN & CATHERINE HASENZAHL, NON-VOLUNTARY LICENSING OF PATENTED INVENTIONS: HISTORICAL PERSPECTIVE, LEGAL FRAMEWORK UNDER TRIPS, AND AN OVERVIEW OF THE PRACTICE IN CANADA AND THE UNITED STATES OF AMERICA 13 nn.92-93 (2002) (describing the experiences of Brazil and the United States in using the threat of compulsory licensing to drive down the prices of AIDS drugs), *available at* http://www.ictsd.org/iprsonline/unctadictsd/docs/reichman_hasenzahl.pdf (last visited July 19, 2003); *Patent Remedies*, ECONOMIST, Oct. 25, 2001 (stating that the U.S. Department of Health used the specter of domestic compulsory licensing to obtain a half-price discount on Cipro from Bayer), 2001 WL 7320684; Tina Rosenberg, *Look at Brazil*, N.Y. TIMES, Jan. 28, 2001 (detailing how Brazil effectively used the threat of compulsory licensing to leverage discounted prices on AIDS drugs), http://www.nytimes.com/library/magazine/home/20010128mag-aids.html (last visited July 19, 2003).

8. *See* Tren, *supra* note 2, at A10.

In five of the six cases I studied, I observed no measurable decline in innovation. This finding is consistent with earlier work. By available measures, the companies affected by licenses continued to perform research and development ("R&D") in the therapeutic areas targeted by the license. Even in the case of forward-looking compulsory licenses that spanned several years, the decline in R&D that advocates for strong patent rights might predict was not observed. While limited and anecdotal, this and past work suggest that concerns about compulsory licensing are overstated and that the blanket assertion that licensing categorically harms innovation is probably wrong.

This Article also discusses how the structure and implementation of compulsory licenses affects R&D. Based on past research and common sense, I postulated that two factors are extremely important—the degree to which a company can predict that a compulsory license will be taken on a patent ("predictability") and the relative importance of the markets affected by the license ("importance"). In the six cases analyzed, licenses that were either unpredictable or did not affect important markets had no discernable impact on R&D, all other things being equal. In all cases but one, the license was either unpredictable or did not impact a developed, existing product market. I observed no reduction in R&D activity in these cases. However, in the one case where licensing was both predictable and impacted a developed market for a drug, there was some evidence of a decline in R&D. Although too few in number to be conclusive, these cases and earlier work provide hope that compulsory licensing need not discourage innovation. They also underscore that the manner in which compulsory licenses are structured and implemented matters, and suggest that the factors of predictability and market impact deserve special attention.

Part II of this Article provides an overview of compulsory licensing. Part III explores the role of patents in pharmaceutical innovation and discusses the compulsory licensing of drugs. Part IV discusses the existing literature on the impact of compulsory licensing on innovation. Part V reports the results of empirical analyses performed on six case studies of pharmaceutical compulsory licensing. Part VI discusses the implications of these results for policymaking.

II. COMPULSORY LICENSING OVERVIEW

Compulsory licenses are generally defined as "authorizations permitting a third party to make, use, or sell a patented invention without the pat-

ent owner's consent."[9] Because they limit the power conferred by patents, compulsory licenses have long been controversial.[10] This part briefly reviews the origins of compulsory licenses, the arguments for and against them in both the United States and developing countries, and the record of their implementation in the United States.

A. General Overview

The current debate over compulsory licensing is nothing new. In the United States Senate in 1790, in the House of Lords in Britain in 1851, and in Germany in 1853,[11] policy makers discussed compulsory licensing as a way to preserve the benefits of the patent system while minimizing its evils. On the one hand, patents created positive incentives for innovation and the disclosure of inventions, granted "just rewards" to inventors, demonstrated society's recognition of the "natural" property rights of inventors, and generally addressed the public goods problems associated with creation of knowledge.[12] On the other hand, these benefits came at a cost, including the potential abuse of monopoly power by patentees, the use of patents to block inventive activity by third parties, the diversion of productive activity disproportionately towards patentable activity, and the substantial administrative costs of operating a patent system.[13]

With these benefits and costs in mind, patent critics and advocates accepted compulsory licensing as a "strategic compromise" in 1873 at the Patent Congress in Vienna.[14] In order to preserve the incentive for innova-

---

9. *See* SCHERER & WATAL, *supra* note 3, at 12.

10. Although this Article focuses on compulsory licenses in the patent context, these licenses also arise in the context of other intellectual property, such as copyrights. *See* ROBERT A. GORMAN & JANE C. GINSBURG, COPYRIGHT 498-505 (6th ed. 2002) (describing the introduction of compulsory licensing into U.S. copyright law in 1909 and discussing 17 U.S.C. § 115, which permits the taking of licenses to publicly distributed phonorecords without the permission of the copyright holder).

11. *See* FRITZ MACHLUP, STAFF OF SUBCOMM. ON PATENTS, TRADEMARKS, AND COPYRIGHTS OF THE SENATE COMM. ON THE JUDICIARY, 85TH CONG., AN ECONOMIC REVIEW OF THE PATENT SYSTEM 5 (Comm. Print 1958) [hereinafter ECONOMIC REVIEW OF THE PATENT SYSTEM].

12. *See, e.g.*, Machlup & Penrose, *supra* note 4, at 10-11.

13. *See, e.g.*, Michael A. Heller & Rebecca S. Eisenberg, *Can Patents Deter Innovation? The Anticommons in Biomedical Research*, 280 SCI. 698 (1998) (describing the problem of "blocking" patents in biomedical research); Machlup & Penrose, *supra* note 4, at 23-28 (discussing general critiques of the patent system); James Love, *Paying for Health Care R&D: Carrots and Sticks*, Consumer Project on Technology, Oct. 19, 2000, (articulating perceived abuses of the patent system), *at* http://www.cptech.org/ip/health/rnd/carrotsnsticks.html (last visited Aug. 27, 2003).

14. A battle occurred between the anti-patent movement of the 1850s through 1870s and the patent advocates of the 1870s through 1910s: "The strategic compromise was the

tion while increasing access to innovations themselves, the Congress adopted a requirement that licensees pay patent holders reasonable compensation for their licenses.[15] With the subsequent adoption of compulsory licensing by the 1883 Paris Convention,[16] the world's foremost international patent agreement, compulsory licensing became a fixture in almost all patent systems.[17]

While specific provisions vary, compulsory licenses are generally authorized in the event of undesirable behavior by the patentee, such as anticompetitive, non-working, or blocking behavior; in the event of "public need," such as government infringement or national emergency; or in the context of food and drugs.[18] Licensees are commonly required to pay adequate compensation to a patentee in exchange for use of a patent. The required amount is generally more than a "reasonable royalty," the floor for infringement compensation in the United States,[19] but less than "lost profits," another basis for calculating infringement damages.[20] The amount of compensation varies among countries; commentators have observed that "the United Kingdom has provided the most generous compensation in its drug patent licensing decisions; the United States the least generous compensation in key antitrust decisions."[21]

---

acceptance of the principle of compulsory licensing—of compelling all patentees to license others to use the invention at reasonable compensation . . .. The patent advocates and the free traders compromised on this general limitation on the patentees' monopoly power." *See* ECONOMIC REVIEW OF THE PATENT SYSTEM, *supra* note 11, at 5.

15. *Id.*

16. *See* Paris Convention for Protection of Industrial Property, Mar. 20, 1883, art. 5A, 21 U.S.T. 1583 (last revised at Stockholm, July 14, 1967).

17. As of Feb. 13, 2002, 163 states, including most industrialized countries, had ratified the Convention. *See* World Intellectual Property Organization [hereinafter WIPO], *Paris Convention for the Protection of Industrial Property*, *at* http://www.wipo.int/treaties/documents/english/word/d-paris.doc (last visited July 18, 2003).

18. *See, e.g.*, FREDERICK M. ABBOTT, COMPULSORY LICENSING FOR PUBLIC HEALTH NEEDS: THE TRIPS AGENDA AT THE WTO AFTER THE DOHA DECLARATION ON PUBLIC HEALTH (Quaker United Nations Office, Occasional Paper No. 9, 2002); Gianna Julian-Arnold, *International Compulsory Licensing: The Rationales and the Reality*, 33 IDEA 349, 349-55 (1993).

19. 35 U.S.C. § 284 (2000) (stating that the damages for patent infringement "shall [be] . . . adequate to compensate for the infringement, but in no event less than a reasonable royalty for the use made of the invention by the infringer").

20. ROBERT P. MERGES, PATENT LAW AND POLICY 1038-84 (2d ed. 1997).

21. SCHERER & WATAL, *supra* note 3, at 28.

B. United States versus Developing Country Perspectives on Compulsory Licensing

Within the general framework of compulsory licensing, however, there has been little consensus on how best to implement it. In modern times, nowhere has the divergence in views been more pronounced than in the context of the compulsory licensing provisions of TRIPS. This was particularly evident during the negotiations behind these provisions. While the United States viewed these provisions with distrust and suspicion, developing countries claimed them to be an essential part of a workable patent system.[22] Commentators have noted that the resulting provisions, discussed below, were left intentionally vague, reflecting the parties' inability to come to an agreement.[23]

The contrast in views on patents between the United States and developing countries is driven in part by differences in economic status. In developing countries, foreigners file most of the patents.[24] As a result, the

22. During TRIPS negotiations in 1989, the U.S. representative characterized compulsory licensing as prone to "mischievous use," and favored a more restrictive, exceptional regime in which licensing would be permitted only for "legitimate purposes." *Note by the Secretariat, Meeting of Negotiating Group of 12-14 July 1989*, 14.doc, ¶ 83.2, *available at* WTO, http://www.wto.org/english/tratop_e/trips_e/trips_e.htm (download derestricted official document archive under heading *History: Derestricted Uruguay Round Negotiating Documents on TRIPS*) (last visited Aug. 20, 2003). In contrast, India's representative stated that compulsory licensing should be viewed as a means for balancing the rights and obligations of patent holders; compulsory licenses should not be narrowly circumscribed, particularly since they are vital to the transfer of technology. *Id.* ¶ 83.3. This difference in views led to competing draft legislation in 1990. The version supported by the United States and other developed nations narrowly defined the basis for licenses, whereas the version supported by developing countries was much more open-ended. *See generally* ABBOTT, *supra* note 18.

23. *See* JEAN O. LANJOUW, INTELLECTUAL PROPERTY AND THE AVAILABILITY OF PHARMACEUTICALS IN POOR COUNTRIES 25 (Ctr. for Global Dev., Working Paper No. 5, 2002). *But see* REICHMAN & HASENZAHL, *supra* note 7, at 12-13 (stating that the resulting language ultimately vindicated the stance of developing countries over that of the United States).

24. Consider, for example, Brazil and South Africa. These are two developing countries against which U.S. government and industry have initiated significant patent disputes over compulsory licensing. Brazil held less than 0.1% of the U.S. patents issued in 1998, while the United States captured nearly 40% of the patents issued in Brazil that same year. In South Africa, foreigners applied for over 99% of the patents in 1999 (issued patent data is not available), and 40% of those applications were from the United States. In contrast, South African inventors captured less than 0.1% of U.S. patents issued in 1998. *See* 1 NAT'L SCI. BD., SCIENCE & ENGINEERING INDICATORS—2002, source data for 6-21 fig.6-23, source data for 6-25 fig.6-27 [hereinafter NAT'L SCI. BD. SOURCE DATA], *at* http://www.nsf.gov/sbe/srs/seind02/pdf/volume1.pdf (last visited Aug. 24, 2003) (source data for fig.6-23, *at* http://www.nsf.gov/sbe/srs/seind02/c6/fig06-23.xls;

patent system facilitates the transfer of monopoly rents to foreigners outside the country, although it is also true that companies may choose not to patent inventions in markets they regard as too small to be significant.[25] Furthermore, the high price of products covered by patents can put needed technology out of the reach of developing country consumers, who are generally required to pay for drugs out of pocket due to the lack of healthcare infrastructure.[26] To compensate for these patent system costs, permissive compulsory licenses are used to widen distribution of and increase access to patented technologies. The situation is different in the United States since U.S. inventors capture a large share of patents both domestically and abroad.[27] Patent profits from both domestic and international markets reward and support research performed locally by U.S. inventors.

Another basic reason for the difference in perspectives derives from the rationales behind each country's patent system. Generally, countries with relatively few patents view the patent system as a means to promote the transfer of technology from other countries.[28] Compulsory licensing provides an important safeguard to ensure that technology transfer happens in the event of non-working or high prices. In contrast, countries such

---

source data for fig.6-27, *at* http://www.nsf.gov/sbe/srs/seind02/c6/fig06-27.xls); U.S. PAT. & TRADEMARK OFF., PATENTING TRENDS CALENDAR YEAR 1999, *at* http://www.uspto.gov/web/offices/ac/ido/oeip/taf/pat_tr99.htm (last visited Aug. 24, 2003); WIPO, WIPO INDUSTRIAL PROPERTY STATISTICS 1999, WIPO Doc. IP/STAT/1999/B (1999), *at* http://www.wipo.org/ipstats/en/publications/b/1999/i/pattab1.pdf (last visited Aug. 24, 2003).

25. *See* Attaran & Gillespie-White, *supra* note 5, at 1890.

26. *See* WORLD HEALTH ORG. & WORLD TRADE ORG. SECRETARIATS, REPORT OF THE WORKSHOP ON DIFFERENTIAL PRICING AND FINANCING OF ESSENTIAL DRUG [sic] 6 (2001) (reporting that 90% of the population in developing countries buys medicines out-of-pocket, whereas only 20% of the population does so in high income countries), *at* http://www.who.int/medicines/library/edm_general/who-wto-hosbjor/wholereporthosbjorworkshop-fin-eng.pdf (last visited Aug. 24, 2003).

27. In the United States, a thin majority (54%) of patents were granted to U.S. residents in 2001. U.S. PAT. & TRADEMARK OFF., 2001 PERFORMANCE AND ACCOUNTABILITY REPORT 115, 118 (2001), *at* http://www.uspto.gov/web/offices/com/annual/2001/01performreport.pdf. Most of the remaining patents were granted to inventors from developed countries. *Id.* Because U.S. inventors capture an extensive share of the patents in these developed countries, the costs of foreign patenting are counterbalanced by the benefits to U.S. inventors of obtaining patents abroad. In 1998, for instance, the United States captured 45%, 28%, 28%, and 30.4% of the patents awarded to foreigners in Japan, Germany, France, and the United Kingdom, respectively, while the same countries each captured 46%, 14%, 5%, and 5%, respectively, of the patents awarded by the United States to residents of foreign countries. *See* NAT'L SCI. BD. SOURCE DATA, *supra* note 24.

28. *See* Edith Penrose, *International Patenting and the Less-Developed Countries*, 83 ECON. J. 768, 771 (1973).

as the United States claim a relatively large share of the world's patents and look to the patent system primarily as an incentive to innovate and a means to stimulate technology creation.[29] This innovation-based focus leads to the selective application of compulsory licensing to cases where patents hinder rather than advance innovation.

C. Compulsory Licensing in the United States

Consistent with a focus on innovation, the U.S. government has used compulsory licenses to curb anti-competitive behavior.[30] By 1977, the Federal Trade Commission ("FTC") and DOJ had issued approximately 125 decrees over thousands of patents and a wide range of technology.[31] Recently, such decrees have been ordered in the context of mergers, price-fixing, and the abuse of monopoly or market power.[32] Compulsory licensing has also been proposed as a solution to the problem of patent thickets, wherein broad or multiple patents over technology areas prevent follow-on research. Voluntary or compulsory patent pools, in which the rights to use multiple patents are exchanged among patentees have been proposed as a way to overcome the refusal of patentees to license an invention and the administrative burden associated with licensing.[33]

However, compulsory licensing has also been used to further public interests, primarily by enabling the U.S. government to use patented inventions without permission. Although courts have emphatically resisted issuing compulsory licenses merely because a patentee chooses not to use

---

29. *See* Clarisa Long, *Patents and Cumulative Innovation*, 2 WASH. U. J.L. & POL'Y 229, 231 (2000).

30. *See, e.g.*, United States v. Nat'l Lead Co., 332 U.S. 319 (1947); Hartford-Empire Co. v. United States, 323 U.S. 386, 417 (1945); *see also* Arti K. Rai & Rebecca S. Eisenberg, *Bayh-Dole Reform and the Progress of Biomedicine*, 66 LAW & CONTEMP. PROBS. 289, 297 n.46 (2003) (noting the role of the U.S. military in ensuring cross-licenses between the Wright Brothers and follow-on innovators).

31. *See* F.M. SCHERER, THE ECONOMIC EFFECTS OF COMPULSORY PATENT LICENSING 47-48 (1977).

32. *See, e.g.*, *Compulsory Licensing as Remedy to Anticompetitive Practices*, Consumer Project on Technology, *at* http://www.cptech.org/ip/health/cl/us-at.html (last visited July 18, 2003) (reporting that of twenty-five compulsory licenses issued since the mid-90s, roughly half resulted from mergers and acquisitions, while the remainder resulted from other forms of anticompetitive behavior).

33. *See generally* JEANNE CLARK ET AL., U.S. PAT. & TRADEMARK OFF., PATENT POOLS: A SOLUTION TO THE PROBLEM OF ACCESS IN BIOTECHNOLOGY PATENTS? 8-12 (2000) (discussing the use of patent pools as a solution to the problems associated with biotechnology patents), *available at* http://www.uspto.gov/web/offices/pac/dapp/opla/patentpool.pdf (last visited July 19, 2003).

her invention,[34] the U.S. government routinely relies on 28 U.S.C. § 1498 to immunize its use of inventions without the patentee's permission. The statute limits a patentee's remedy for infringement by the government or a government contractor to "reasonable and entire compensation."[35] By not allowing for injunctive relief, the statute effectively strips patentees of the right to prevent others from using their inventions.

Although the statute was originally conceived with wartime urgency in mind,[36] the government has used it in a wide range of circumstances. Since 1948, the year of the statute's enactment in its current form,[37] the Court of Federal Claims and its predecessors have decided almost 300 cases, involving a wide variety of technologies, under § 1498.[38] Although this figure is surprisingly large, it arguably understates the use of compulsory licenses by the government because it excludes cases resolved without litigation and infringement that goes unnoticed by the patentee. In infringement suits against the government that have been decided on the

---

34. *See, e.g.*, Cont'l Paper Bag Co. v. E. Paper Bag Co., 210 U.S. 405, 429 (1908) (holding that "it is the privilege of any owner of property to use or not to use it, without question of motive"); *see also* 35 U.S.C. § 271(d)(4) (2000) (confirming by amendment under the Patent Misuse Reform Act of 1988 that the refusal to license or use one's patents rights does not by itself constitute misuse for which compulsory licensing would be a remedy).

35. 28 U.S.C. § 1498(a). The subsection states:

> Whenever an invention described in and covered by a patent of the United States is used or manufactured by or for the United States without license of the owner thereof or lawful right to use or manufacture the same, the owner's remedy shall be by action against the United States in the United States Court of Federal Claims for the recovery of his *reasonable and entire compensation* for such use and manufacture . . . .

Id. (emphasis added).

36. In *Richmond Screw v. United States*, the Supreme Court commented about the statute:

> The intention and purpose of Congress . . . was to stimulate contractors to furnish what was needed for the war, without fear of becoming liable themselves for infringements to inventors or the owners or assignees of patents . . . . To accomplish this governmental purpose, Congress exercised the power to take away the right of the owner of the patent to recover from the contractor for infringements.

275 U.S. 331, 345 (1928).

37. *See* Lionel Marks Lavenue, *Patent Infringement Against the United States and Government Contractors Under 28 U.S.C. § 1498 in the United States Court of Federal Claims*, 2 J. INTELL. PROP. L. 389, 415 (1995).

38. *Id.* at 496 n.563 (noting that there have been 240 cases from 1949 to Apr. 1, 1994); LEXIS search, Genfed Library, FED File (Apr. 2, 1994 through Aug. 10, 2002) using search terms "28 U.S.C. § 498", "government", and "patent."

merits, plaintiff patentees have won just over one-third of the time,[39] as compared to a 58% success rate of patentees against accused infringers in general.[40] Outside the context of section 1498, compulsory licenses have been authorized for public policy reasons, but on a more limited scale.[41]

III. THE COMPULSORY LICENSING OF DRUGS

Against the backdrop of compulsory licensing, this part discusses the role of patents in drug innovation and the compulsory licensing of drugs both in the United States and under TRIPS.

A. Patents and Drug Innovation

Drugs have been singled out for special treatment both in terms of patenting and compulsory licensing primarily because of their role in promoting public health. For many years product patents were not awarded over pharmaceuticals. In the developed world, Japan did not introduce product patents for drugs until 1976, and pharmaceutical powerhouse Switzerland waited until 1977 to introduce patents covering pharmaceutical products.[42] Spain, Portugal, Greece, and Norway introduced product patents over drugs as recently as 1992.[43] At the end of the 1980s, at least forty developing countries, including the most populous, provided no patent protection for pharmaceuticals.[44] The rationale behind this policy of non-protection

39. This figure is based on an analysis of cases from 1982 to 1993. *See* Lavenue, *supra* note 37, at 502.

40. Kimberly A. Moore, *Judges, Juries, and Patent Cases—An Empirical Peek Inside the Black Box*, 99 MICH. L. REV. 365, 385 (2000).

41. *See* 42 U.S.C. § 2183 (2000) (allowing the Atomic Energy Commission to compel licensing of certain "public interest" patents); *id.* § 7608 (allowing compulsory licenses if use of the patented invention is required to meet emission requirements, no reasonable alternative is available to meet the requirements, and the lack of availability of the patentee would tend to lessen competition). In several cases, courts have *de facto* authorized compulsory licensing by rewarding damages but refusing to enjoin infringement for public interest reasons. *See* Vitamin Technologists v. Wis. Alumni Research Found., 146 F.2d 941 (9th Cir. 1945) (stating that the partial refusal to license production of vitamin D in oleomargarine amounted to patent misuse and suggesting that an injunction could be denied if the refusal to license was against public interest); Milwaukee v. Activated Sludge, Inc., 69 F.2d 577 (7th Cir. 1934) (declining to issue an injunction against a patent infringing sewage plant because it would cause lake pollution), *cert. denied*, 293 U.S. 576 (1934).

42. JEAN O. LANJOUW & IAIN COCKBURN, DO PATENTS MATTER? EMPIRICAL EVIDENCE AFTER GATT 1 n.2 (Nat'l Bureau of Econ. Research, Working Paper No. 7495, 2000).

43. *Id.*

44. *Id.* at 1. However, all WTO members are obligated to offer pharmaceutical patent protection by 2016. *See* ABBOTT, *supra* note 18, at 11.

was that drugs are too important to patent and leave vulnerable to monopoly abuses.

However, a competing rationale has stimulated the recent trend toward granting patent protection for drugs. Drug development is enormously time-consuming, risky, and expensive,[45] intensifying the importance of the patent incentive. In addition, drug patents tend to be more effective in securing commercial advantage because, once invented, drugs are relatively easy to copy, and because a few key patents usually cover a single drug product.[46] Accordingly, surveys published in 1986 and 2000 all concluded that the pharmaceutical, biotechnology, and chemical industries rely more heavily on patents than other industries.[47] Pointing to these facts, critics of compulsory licensing have concluded that drugs are too crucial *not* to be protected by patents.

The U.S. system reflects this inherent tension, extensively regulating drug development on one hand and providing special incentives for drug innovation on the other. In terms of regulation, pharmaceutical companies must undergo a lengthy drug approval process administered by the Food

---

45. Precisely how expensive is highly contested. Researchers at Tufts estimate the cost of developing a new drug to be $802 million. Joseph A. DiMasi et al., *The Price of Innovation: New Estimates of Drug Development Costs*, 22 J. HEALTH ECON. 151, 166 (2003). However, roughly half of this figure reflects opportunity costs within the industry. *Id.* Using data from PhRMA, Public Citizen estimates the cost of development to be between $114 million and $150 million. PUBLIC CITIZEN, RX R&D MYTHS: THE CASE AGAINST THE DRUG INDUSTRY'S R&D "SCARE CARD" 7 (2001), *available at* http://www.citizen.org./documents/acfdc.pdf (last visited Aug. 27, 2003). The Boston Consulting Group, who estimates a development cost of $880 million, suggests that $165 million is spent in target identification, $205 million is spent on target validation, $40 million is spent on screening, $120 million is spent on optimization, $90 million is spent on preclinical development, and $260 million on clinical development. The time expended in each of these phases is estimated at 1, 2, 0.4, 2.7, 1.6, and 7 years, respectively. *See* PETER TOLLMAN ET AL., THE BOSTON CONSULTING GROUP, A REVOLUTION IN R&D: HOW GENOMICS AND GENETICS ARE TRANSFORMING THE BIOPHARMACEUTICAL INDUSTRY 12 (2001), *available at* http://www.bcg.com/publications/files/eng_genomicsgenetics_rep_11_01.pdf.

46. *See* F.M. Scherer, *The Pharmaceutical Industry and World Intellectual Property Standards*, 53 VAND. L. REV. 2245, 2247 (2000) (estimating that it costs only $1 million to copy a drug); *cf.* DiMasi, *supra* note 45 (estimating the development cost of a new pharmaceutical to be $802 million).

47. This difference in reliance on patents is decreasing. *See* WESLEY M. COHEN ET AL., PROTECTING THEIR INTELLECTUAL ASSETS: APPROPRIABILITY CONDITIONS AND WHY U.S. MANUFACTURING FIRMS PATENT (OR NOT) 11-14 (Nat'l Bureau of Econ. Research, Working Paper No. 7552, 2000), *available at* http://papers.nber.org/papers/w7552.pdf (last visited Aug. 27, 2003); Edwin Mansfield, *Patents and Innovation: An Empirical Study*, 32 MGMT. SCI. 173, 175 (1986).

and Drug Administration ("FDA") prior to selling a new drug to the public. Companies must prove the efficacy and safety of the new drug. Direct-to-consumer drug advertising, liberalized in 1997, remains heavily regulated.[48] The government has occasionally authorized or ordered the compulsory licensing of patented drugs as well, as discussed below.

In terms of incentives, the Orphan Drug Act of 1983 provides marketing exclusivity, tax incentives, and research grants for companies engaging in research on rare "orphan" diseases that affect a small share of the population.[49] Similarly, the Hatch-Waxman Act of 1984 extends the period of exclusivity granted by drug patents in order to compensate for time lost in FDA approvals.[50] These extensions are meant to encourage not only the initial R&D that leads to the discovery of patentable drug inventions, but the expensive and time-consuming testing and commercialization of inventions after their discovery. In fact, according to one estimate, close to 50% of expenditures take place post-patenting.[51] Although post-patenting development activities are highly worthwhile and for all practical purposes required in order for the public to benefit from the patented innovation, they are not necessarily "innovative" in the sense typically thought of, especially given that they are carried out downstream from the patentable invention, often by parties other than the inventor.[52]

B. Compulsory Licensing of Drugs in the United States

To date, Congress has resisted enacting specific provisions authorizing the compulsory licensing of drugs, although pharmaceutical-specific price

48. *See* Tamar V. Terzian, *Direct-to-Consumer Prescription Drug Advertising*, 25 AM. J.L. & MED. 149 (1999) (describing the FDA's in-depth regulations of prescription drug broadcast advertisements).

49. *See, e.g.*, F.M. Scherer, *Pricing, Profits, and Technological Progress in the Pharmaceutical Industry*, 7 J. ECON. PERSP. 97 (1993) [hereinafter Scherer, *Pricing*].

50. *See* THE BOSTON CONSULTING GROUP, SUSTAINING INNOVATION IN U.S. PHARMACEUTICALS: INTELLECTUAL PROPERTY PROTECTION AND THE ROLE OF PATENTS 16-18 (1996).

51. TOLLMAN ET AL., *supra* note 45 and accompanying text. In the Boston Consulting Group model, it is assumed that there are eleven years of patent protection after clinical development. *Id.* at 59-60. Based on a patent life of twenty to twenty-three years, after Hatch-Waxman extensions, this means that patents are issued nine to twelve years before FDA approval, before the time consuming clinical and development phases, which consume 45% of total expenditures. *See* The Boston Consulting Group, *supra* note 50, at 35 (stating that average extensions are two to three years in length).

52. *See generally* DATAMONITOR, REP. NO. DMHC1554, CREATING WIN-WIN BIOTECHNOLOGY AND PHARMACEUTICAL DEALS 22 (Oct. 2000) (describing the various ways in which biotechnology firms may license their inventions to pharmaceuticals in the development phase and estimating that 30% of pharmaceuticals use portfolio management, a strategic tool that specifically contemplates drug development partnerships).

regulation has been contemplated intermittently since the 1950s. In the late 1950s and early 1960s, the Kefauver hearings turned public scrutiny on the industry's above-average profit levels, price markups, false and misleading advertising, and general lack of price competition.[53] In 1962, Congress enacted the Kefauver-Harris amendments, which increased the FDA's involvement in the development and advertising of drugs.[54] U.S. lawmakers again addressed price control mechanisms in 1972 with the proposal of the Public Health Price Protection Act, which was ultimately unsuccessful.[55]

During the 1990s, several trends came together to focus attention on drug pricing, the most prominent being the "relentless escalation" of health care costs.[56] By 1992, the United States devoted 14% of its Gross National Product to healthcare costs, more than any other industrialized country.[57] Prices rose much faster on drugs than on other goods, and pharmaceutical profitability levels topped those of all other industries.[58] The unsuccessful Hart Bill of 1993 and Affordable Prescription Drugs Act of 1999 proposed compulsory licensing of health related patents in various circumstances, such as unreasonable pricing.[59] In 2000 and 2002, President Clinton and President Bush, respectively, blocked the implementation of bills that would have enabled prescription drug wholesalers to import drugs from countries where they are cheaper.[60]

As another form of price regulation, compulsory licenses over drug patents have been granted in two contexts—under 28 U.S.C. § 1498 and under antitrust consent decrees. Although few in number, drug licenses taken pursuant to the statute have involved deliberate infringement by the

---

53. *See* Mary T. Griffin, *AIDS Drugs & the Pharmaceutical Industry: A Need for Reform*, 17 AM. J.L. & MED. 363, 377 (1991).

54. *Id.*

55. *Id.* at 404.

56. Scherer, *Pricing*, *supra* note 49, at 97.

57. *Id.*

58. *Id.* at 98.

59. *See* Joseph A. Yosick, *Compulsory Patent Licensing for Efficient Use of Inventions*, 2001 U. ILL. L. REV. 1275, 1278 (2001).

60. *See* Mason Essif, *Prescription Drugs are Crossing Borders to Buyers*, CNN.COM, Mar. 12, 2001, *at* http://www.cnn.com/2001/HEALTH/03/12/prescription.drugs (last visited Aug. 1, 2003); Robert Pear, *Plan to Import Drugs From Canada Passes In Senate, but Bush Declines to Carry It Out*, N.Y. TIMES, July 18, 2002, *available at* 2002 WL 24463223. *But see Import Drug Bill Clears House*, CBSNEWS.COM, July 25, 2003, *at* http://www.cbsnews.com/stories/2003/07/25/politics/main565066.shtml (last visited Aug. 11, 2003) (describing House passage of a bill that allows for importation of drugs from Canada and the European Union and that, unlike past bills, specifically avoids presidential oversight of the drug approval process).

government to produce drugs for public health purposes. In the 1960s and 1970s, the U.S. government made and used tetracycline[61] and meprobamate[62] for the military without permission from patent holders. Similarly, in the fall of 2001, the threat of a compulsory license was used to drive down the price of the patented drug Cipro by almost 50%.[63]

Antitrust orders have generated many more compulsory licenses, and have been issued to remedy patent misuse and the use of patents in price-fixing, entry-restricting cartels, and market concentration schemes.[64] One of the most notable early cases involved the licensing of tetracycline, ampicillin, and related products as part of a judgment against Pfizer, American Cyanimid, and other pharmaceutical companies, in response to an antibiotic price-fixing scheme.[65]

In the 1970s, the FTC created a division, staffed with thirty-five lawyers and investigators within the Bureau of Competition, to work exclusively on health care antitrust issues.[66] In the second half of the 1980s and early 1991, in response to the rising number of pharmaceutical mergers, the division issued twelve consent decrees. Five decrees involved horizontal mergers between direct competitors, three involved mergers between potential competitors, and four involved the proposed combination of R&D "innovation" markets.[67] Six of the twelve decrees ordered the compulsory licensing of patented drugs; these form the basis of the analysis in Part IV.

Although all antitrust licensing orders seek to address antitrust concerns, their provisions have varied, depending on whether their objective was to increase access to existing competitors, facilitate entry of new competitors, or redress past wrongs by the patentee. Under a decree, remuneration for licenses may be negotiated by the parties, set by the court,

---

61. *See* SCHERER & WATAL, *supra* note 3, at 26.

62. Carter-Wallace, Inc. v. United States, 496 F.2d 535 (Ct. Cl. 1974).

63. *See* Kavaljit Singh, *Anthrax, Drug Transnationals, and TRIPs*, FOREIGN POLICY IN FOCUS NEWSLETTER, Apr. 29, 2002, at 1-3, *available at* http://www.fpif.org/pdf/gac/OUS0204trips.pdf (last visited Aug. 8, 2003); Press Release, U.S. Dep't Health & Human Servs., HHS, Bayer Agree To Cipro Purchase (Oct. 24, 2001), *available at* http://www.hhs.gov/news/press/2001pres/20011024.html (last visited Aug. 8, 2003).

64. SCHERER & WATAL, *supra* note 3, at 17.

65. *See In re* Am. Cyanamid Co., 63 F.T.C. 1747 (1963); Peter Temin, *Technology, Regulation, and Market Structure in the Modern Pharmaceutical Industry*, 10 BELL J. ECON. 429, 435-41 (1979).

66. *See* HEALTHCARE SERVS. & PRODS. DIV., FED. TRADE COMM'N, FTC ANTITRUST ACTIONS IN HEALTHCARE SERVICES AND PRODUCTS 1-2 (Apr. 2003), *available at* http://www.ftc.gov./bc/hcupdate030401.pdf.

67. *Id.*

or set at zero (royalty-free). Most often, orders call for reasonable royalties and let the parties decide on the price. The court only intervenes if the parties cannot agree. Some orders indicate specific monetary licensing terms, while others authorize cross-licenses as an alternative.[68] Royalty-free licenses are issued more rarely—usually in cases of misconduct.[69]

Additionally, to ensure that the license issues to a viable or prospective competitor, the DOJ or FTC approval of the licensee and additional license terms is sometimes required.[70] Also, to increase the likelihood that patents will be used efficiently, the license may cover know-how, manufacturing capability, or other tangible or intangible assets in addition to the patents. Special precautions are often taken in the case of pharmaceutical licenses because of the special challenges posed by the time-consuming and expensive drug development process.[71] This has led to the creation of additional obligations for the patentee, such as providing ongoing support until the licensee's product is approved, and the possibility of a continuing relationship with the licensee.

C. Compulsory Licensing of Drugs under TRIPS

TRIPS contains a comprehensive framework for the compulsory licensing of patented inventions. The agreement also makes clear that, for public health reasons, countries may suspend patent protection over drugs.

The primary provision for compulsory licensing is Article 31, which is entitled "Other Use without Authorization of the Right Holder." This pro-

---

68. *See, e.g.*, Hartford-Empire Co. v. United States, 323 U.S. 386, 414-17 (1945).

69. *See, e.g.*, Lawrence Schlam, *Compulsory Royalty-Free Licensing as an Antitrust Remedy for Patent Fraud: Law, Policy and the Patent-Antitrust Interface Revisited*, 7 CORNELL J.L. & PUB. POL'Y 467 (1998).

70. *See In re* Institut Merieux S.A., 113 F.T.C. 742 (1990).

71. *See* BUREAU OF COMPETITION, FED. TRADE COMM'N, A STUDY OF THE COMMISSION'S DIVESTITURE PROCESS 40-41 (1999), *available at* http://www.ftc.gov/os/1999/08/divestiture.pdf (last visited Aug. 28, 2003). The study stated that:

> The pharmaceutical orders played an important role in the development of the divestiture remedies because they posed, in a more obvious form, some of the difficulties found in the Study. . . . Foremost among them is the fact that divestiture is not possible unless the Food and Drug Administration authorizes the buyer to produce the drug or health product. Until approval is obtained, the most that the buyer could expect to do under FDA rules is to market and distribute the products made by the respondent. In the meantime, the buyer would be required to build and replicate exactly the respondent's production facilities. The orders had to reflect these realities through provisions requiring interim supply agreements and technical assistance for a substantial period of time.

Id.

vision permits WTO member countries to authorize compulsory licenses for use by the government or third parties subject to certain restrictions. Under all circumstances, patentees are to receive "adequate remuneration . . . taking into account the economic value of the authorization."[72] Before licenses are granted, the proposed user must try unsuccessfully for a reasonable amount of time to secure a license on reasonable terms.[73] However, this requirement is waived if there is "a national emergency" or a "circumstance[] of extreme urgency," or if the patented invention is used for "public noncommercial use."[74] Such use must be non-exclusive and non-assignable.[75] Additionally, unless the patentee has engaged in anti-competitive behavior, the use must predominately supply the domestic market.[76] Finally, the scope and duration of use is limited to the purpose authorized with a license subject to termination "if and when the circumstances which led to it cease to exist and are unlikely to recur."[77] Article 30 authorizes general exceptions to patent protection, presumably including compulsory licensing, but states that these exceptions must neither "unreasonably conflict with a normal exploitation of the patent" nor "unreasonably prejudice the legitimate interests of the patent owner."[78]

While Articles 30 and 31 apply to patents in all fields, Articles 8 and 27, as well as the Doha Declaration on the TRIPS Agreement and Public Health ("Doha Declaration"), explicitly address the relationship between TRIPS and public health. Article 8 states that "[m]embers may . . . adopt measures necessary to protect public health," but adds the requirement that "such measures are consistent with the provisions of this Agreement."[79] Article 27 allows member countries to exclude from patentability inventions needed to protect public health.[80] The Doha Declaration on TRIPS, adopted in October 2001 by the WTO Ministerial Conference, affirms that countries may undertake compulsory licensing for public health reasons. Heralded as a major step forward in paving the way for cheap drugs for the poor,[81] it states in part:

---

72. TRIPS Agreement art. 31(h).
73. *Id.* art. 31(b).
74. *Id.*
75. *Id.* art. 31(d)-(e).
76. *Id.* art. 31(f), (k).
77. *Id.* art. 31(g).
78. *Id.* art. 30.
79. *Id.* art. 8(1).
80. *Id.* art. 27(2).
81 . *See, e.g.*, Ellen 't Hoen, *TRIPS, Pharmaceutical Patents, and Access to Essential Medicines: A Long Way from Seattle to Doha*, 3 CHI. J. INT'L L. 27, 28 (2002) (describing

> We stress the importance we attach to implementation and interpretation of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) in a manner supportive of public health, by promoting both access to existing medicines and research and development into new medicines and, in this connection, are adopting a separate declaration.[82]

In addition, the Doha Declaration clarifies that member countries may define for themselves "what constitutes a national emergency or other circumstances of extreme urgency."[83] When a country declares an emergency in good faith, this waives the obligation to negotiate under Article 31(b) before issuing a compulsory license. Finally, the Declaration acknowledges the problems imposed by Article 31's requirement that manufacturing be done primarily to service the domestic market, which prevents countries without generic drug manufacturing capabilities from making use of the provision.[84]

While developing countries have pressed for a broad interpretation of the Doha Declaration, and thus a large list of diseases for which patent rules will be relaxed, drug companies and their respective governments have advocated for a narrow interpretation of the Declaration.[85] Although the Declaration required that the TRIPS Council find an "expeditious solu-

---

the Declaration as an "important achievement" that "broke new ground in guaranteeing Members' access to medical products").

82. WTO, Ministerial Declaration, Fourth Ministerial Conference in Doha, Qatar, ¶ 17 (adopted Nov. 14, 2001).

83. *See* WTO, Declaration on the TRIPS Agreement on Public Health, Fourth Ministerial Conference in Doha, Qatar, ¶ 5(c) (adopted Nov. 14, 2001) [hereinafter Doha Declaration].

84. *Id.* ¶ 6. The Doha Declaration states

> [w]e recognize that WTO members with insufficient or no manufacturing capacities in the pharmaceutical sector could face difficulties in making effective use of compulsory licensing under the TRIPS Agreement. We instruct the Council for TRIPS to find an expeditious solution to this problem and to report to the General Council before the end of 2002.

Id.

85. *See, e.g.*, Sarah Boseley & Charlotte Denny, *Prescription for World's Poorest Stays Unwritten: WTO Conference Deadlock as US Shows no Sign of Loosening Veto on Pharmaceutical Patent Rights*, GUARDIAN, Feb. 20, 2003, *available at* http://www.economist.com/agenda/displayStory.cfm?story_id=1589657 (last visited July 19, 2003); *Negotiators Meet Again; Minds Don't*, ECONOMIST, Feb. 19, 2003, *available at* http://www.economist.com/agenda/displayStory.cfm?story_id=1589657 (last visited July 19, 2003).

tion" to these issues by the end of 2002,[86] it was not until late August 2003 that an accord was reached.[87]

IV. EMPIRICAL BACKGROUND (LITERATURE REVIEW)

One major obstacle to the widespread use of compulsory licenses has been the perception that licenses reduce the incentive for innovation offered by the patent system.[88] Insofar as patents are needed to induce innovation, the argument goes, weakening patents through compulsory licenses will reduce innovation. This notion has special import for the drug industry.

First, it is often repeated that drugs, due to the costs and risks associated with drug development, are different than other inventions, and that the drug industry relies on patents more than other industries.[89] Because of this unique dependence on patents, more is at stake for the drug industry than for other industries when measures that reduce patent protection such as compulsory licensing are contemplated.

Second, in light of the current public health crisis, relaxation of patent rules will likely take place to some degree, regardless of any potential effect on innovation.[90] In the context of the AIDS crisis and public health generally in developing countries, at least two kinds of incentives are relevant—those that prompt research in diseases of common interest to developed and developing countries (e.g., AIDS), and those that encourage research in areas specifically relevant to developing countries (e.g., malaria).[91] Particularly problematic could be a negative impact on R&D specific to the developing countries, the growth of which is anxiously anticipated with the introduction of stronger patent protection.[92] In light of these

---

86. Doha Declaration, *supra* note 83, ¶ 6.

87. *See, e.g.*, Elizabeth Becker, *Poor Nations Can Purchase Cheap Drugs Under Accord*, § 1, at 14.

88. *See* Tren, *supra* note 2.

89. *See* Richard C. Levin et al., *Appropriating the Returns from Industrial Research and Development*, 1987 BROOKINGS PAPERS ON ECON. DEV. 783, 796-98 (1987); *supra* note 47.

90. *See infra* note 80 and accompanying text.

91. *See* Jean O. Lanjouw, A Patent Policy Proposal for Global Diseases (Apr. 2001), *at* http://econ.worldbank.org/files/1733_lanjouw.pdf (last visited July 14, 2003).

92. *See generally* CARSTEN FINK, HOW STRONGER PATENT PROTECTION IN INDIA MIGHT AFFECT THE BEHAVIOR OF TRANSNATIONAL PHARMACEUTICAL INDUSTRIES (World Bank Group, Policy Research Working Paper No. 2352, 2000) (modeling the impact of stronger patent rights on the pharmaceutical industry in India), *at* http://www-wds.worldbank.org/servlet/WDSContentServer/WDSP/IB/2000/06/27/000094946_00060905463269/Rendered/PDF/multi_page.pdf (last visited July 28, 2003); LANJOUW &

incentives, the challenge for policy makers will be to implement patent-weakening schemes that increase access but cause minimal harm to the patent innovation incentive.

A. Compulsory License Design

The impact of a license on the licensor's innovation depends on a variety of factors. The following paragraphs identify possible factors that might determine how much a compulsory license impacts innovation.

It is clear that the price at which a compulsory license is set will determine whether and how much innovation is affected. If a compulsory license is priced essentially at what a patentee demands, there is no real reason to anticipate that innovation will be substantially harmed. On the other hand, a compulsory license whose price is set at a level far below market could operate to effectively strip the patentee of its right to any monopoly profits.[93] Besides price, two factors that deserve special attention are "market significance," or the extent to which a licensee actually threatens the patentee's markets, and "predictability," or the extent to which a licensor anticipates a compulsory license.

As to market significance, compulsory licenses can vary in degree as to the competitive threat they pose to licensors. If a compulsory license covers a known product in a licensor's target market, the licensor and the licensee will have to share the same market. Under the above definition, the market significance of this license is high because the licensor's market is directly threatened. Conversely, if the license covers a market that is unimportant to the licensor, or it covers a product that has yet to be proven or for which the market is immature or untested, there is a good chance that the licensee and licensor will not compete head to head. The significance of this license may be relatively low.

Whether a license is predictable is also an important characteristic. Unpredictable licenses that cover only existing technologies are more limited in scope than those that are predictable and cover future inventions. Although the unanticipated loss of exclusivity that accompanies an unpredictable compulsory license may influence a company's decisions about investing in follow-on innovation, development, and commercialization,

---

COCKBURN, *supra* note 42, at 3-4 (establishing for future reference the current baseline of research efforts devoted to those diseases specific to developing countries).

93. For a deeper analysis of the ethical and economic issue of what developing countries should contribute to innovation, see WILLIAM JACK & JEAN O. LANJOUW, FINANCING PHARMACEUTICAL INNOVATION: HOW MUCH SHOULD POOR COUNTRIES CONTRIBUTE? (Ctr. for Global Dev., Working Paper No. 28, 2003), *at* http://www.cgdev.org/wp/cgd_wp028.pdf (last visited Aug. 8, 2003).

the licensing event may come at a point that is too late for the company to change course. This is not the case with an order that requires licensing of future patents. The licensor may choose to redirect R&D investment, put off inventive activity until the license has expired, or choose trade secret over patent protection.

B. Literature Review

For some time, researchers have not focused on compulsory licensing and the more general phenomenon of weakening patent protection, presumably because changes to the patent system over the last several decades have been in the direction of strengthening patent protection.[94] Nevertheless, major studies conducted in the 1960s and 1970s on compulsory licensing regimes concluded that, as implemented, licensing had no long-term negative impact on licensor innovation.[95] The most thorough study to date, which focused on U.S. antitrust consent decrees issued during the 1950s and 1960s, found that licensing had no measurable impact on future innovation in any of the industry segments studied, including pharmaceuticals.[96] Another major study that focused on Canada's extensive general compulsory licensing program similarly concluded that Canada's program had no negative impact on pharmaceutical innovation.[97]

However, research on related questions suggests that some forms of compulsory licensing could be detrimental to innovation. From 1967 to 1968, the Harbridge House conducted a study of civilian utilization of inventions created for the government. The study demonstrated that the loss of exclusivity due to the compulsory licensing of some of the inventions negatively affected utilization rates of those inventions.[98] In addition, there is a perception that compulsory licensing can discourage R&D. A survey of British pharmaceutical executives suggested that they believed that, in some extreme forms, licensing could harm innovation.[99]

Like the study in this Article, these studies focused exclusively on licensor innovation, and largely ignored the impact of compulsory licensing on the licensee. The licensee often benefits from the "spillover" effects of

---

94. *See* LANJOUW & COCKBURN, *supra* note 42.

95. *See* SCHERER, *supra* note 31; Donald G. McFetridge, *Intellectual Property, Technology Diffusion, and Growth in the Canadian Economy*, *in* COMPETITION POLICY AND INTELLECTUAL PROPERTY RIGHTS IN THE KNOWLEDGE BASED ECONOMY 65 (Robert D. Anderson & Nancy T. Gallini eds., 1998).

96. *See* SCHERER, *supra* note 31, at 67-75.

97. *See* McFetridge, *supra* note 95.

98. *See* SCHERER, *supra* note 31, at 78-82.

99. C.T. TAYLOR & Z.A. SILBERSTON, THE ECONOMIC IMPACT OF THE PATENT SYSTEM 198-99 (1973) (study results further described in SCHERER, *supra* note 31, at 60-62).

the original innovation.[100] Indeed, follow-on innovation by competing licensees or by potential entrants is often the very aim of licensing orders in the antitrust context.[101] The question of whether a potential tradeoff between increased licensee innovation and decreased licensor innovation exists, however, is beyond the scope of this Article.

1. Compulsory Licensing under U.S. Antitrust Consent Decrees

In 1977, F.M. Scherer conducted a major study of antitrust, consent-related compulsory licenses. His study focused on nearly seven hundred companies, forty-two of which had been subject to compulsory licenses.[102] Scherer calculated the ratio of each company's R&D expenditures to its sales for the year 1975, and compared ratios between companies that had been subject to significant compulsory licensing decrees and those that had not. Scherer further modeled the relationship between compulsory licensing and R&D, and found a slight positive correlation between licensing and high R&D-to-sales ratios. On average, companies subjected to compulsory licensing actually spent more on R&D than similar firms in their industry that had not been subjected to compulsory licenses.[103] This was true for all industries, including pharmaceuticals. Because Scherer only had data from one year, he was not able to determine whether the R&D expenditures of the firms affected by compulsory licensing had fallen from previously higher levels.[104] Nevertheless, he concluded that compulsory licensing had not forced firms to invest in R&D at a level below the norms in their industries.[105]

---

100. *See* Testimony of the Biotechnology Industry Organization Before the Federal Trade Commission and the Department of Justice, at 2 (Feb. 26, 2002), *available at* http://www.bio.org/ip/pdf/ftc022002.pdf (last visited Aug. 8, 2003).

101. *See* Susan DeSanti, The Intersection of Antitrust and Intellectual Property Issues: A Report from the FTC Hearings, Remarks for the Business Development Association Conference on Antitrust for High-Tech Companies (Feb. 2, 1996), *available at* http://www.ftc.gov/speeches/other/desanti1.htm.

102. *See* SCHERER, *supra* note 31, at 67-68, 74.

103. *Id.* at 75 ("To sum up, the analysis of 1975 research and development spending patterns provides no significant indication that 44 companies subjected to compulsory patent licensing under antitrust decrees sustained less intense R&D efforts than other firms of comparable size and industry origin. If anything the opposite tendency is revealed.").

104. In an earlier survey of thrity-eight companies affected by compulsory licenses, Scherer observed a statistically significant decline in patenting by companies. Based on interviews, he concluded that this was due to a statistical fluke or shift toward trade secrecy. *Id.* at 66-67.

105. *Id.* (observing a statistically significant simple average decline of 15% in absolute patenting).

Scherer's study focused on antitrust licensing decrees. These decrees mandated compulsory licensing as part of case settlements.[106] The majority of these licenses did not require future licensing of patents issuing from the year studied, but covered past inventions.[107] Although Scherer hypothesized that specific past experience with compulsory licenses or the general threat of licenses might produce an adverse impact on R&D behavior, he found no statistical results to support these hypotheses.[108] In the short-term, the largely unpredictable licenses studied did not appear to impact behavior in the year studied. The view that firms focused on the long-term was expressed in an earlier study conducted by Scherer that focused on companies that either had been or were on the verge of being forced to license patents in the antitrust context.[109] The most common explanation provided by the firms for not changing R&D was their long-term interest in the impacted business, and the view that they needed to continue R&D in order to stay competitive.[110]

2. Compulsory Licensing of Drugs in Canada

While the short-term, unpredictable nature of the antitrust licenses studied by Scherer may explain in part why he observed no negative impact on innovation, Canada's experience with compulsory licensing provides a useful example of the opposite extreme—completely predictable licenses.[111] From 1923 to 1993, Canadian legislation authorized compulsory licensing over medicines under sections 4(1) and 39(4) of the Canadian Patent Act. Canada's policy of issuing compulsory licenses for drugs became so routine that it led to the development of a domestic generic drug industry.[112]

In 1985, the Eastman Commission reported the effects of Canada's broad compulsory licensing system on innovation, focusing especially on the pharmaceutical industry.[113] From 1969 to 1983, the period studied by the Commission, almost 80% of the applications for licenses were granted,

106. *Id.* at 63 (describing compulsory licensing in antitrust decrees generally).
107. *Id.* at 69.
108. *Id.* at 69, 74.
109. *Id.* at 62-63.
110. *Id.* at 62.
111. *See* REICHMAN & HASENZAHL, *supra* note 7, at 18-20.
112. *See* SCHERER, *supra* note 31, at 83. The Canadian Parliament abolished the program in 1993 after intense lobbying by the U.S. government during NAFTA negotiations. Objecting vigorously to Canada's broad embrace of compulsory licensing, the U.S. government feared that other countries might follow suit. *See* REICHMAN & HASENZAHL, *supra* note 7, at 21-22.
113. *See* McFetridge, *supra* note 95, at 83.

resulting in an average of approximately twenty compulsory licenses per year.[114] Comparing R&D intensities in Canada to intensities in other small, developed countries, the Commission concluded that compulsory licensing did not significantly affect innovation in Canada.[115]

One reason for this result may be the relative insignificance of the Canadian market to the worldwide market for pharmaceuticals. Researchers noted that for the most part, "Canadian R&D . . . expenditures constitute[d] a very small fraction of [corporate parent] R&D and . . . remain[ed] below the minimum efficient scale for in-house R&D in this industry."[116] As a result, the lack of patent protection in Canada had little influence on R&D decisionmaking.

Thus the Scherer and Eastman Commission studies both concluded that compulsory licensing had little adverse impact on licensor innovation, but probably for different reasons. In the case of U.S. antitrust licenses, the unpredictability and short-term nature of the licenses may explain why they did not greatly affect innovation. In the case of Canadian drug licenses, the relative insignificance of the Canadian market may have accounted for the lack of a noticeable adverse impact.

3. Licensing of U.S. Government Inventions

In contrast to the Eastman and Scherer studies, a study conducted by Harbridge House reported that in some cases, a loss of patent rights might result in negative effects on innovation and commercialization. In the 1960s, the Federal Council for Science and Technology commissioned Harbridge House to investigate whether or not contractors based their decision to commercialize inventions they made for the government on exclusivity grounds.[117] Under the contracts studied, when a contractor created a patented invention for the U.S. government, the government could either take a license to the invention or take title to the invention itself. When the government merely took a license, the contractor had exclusive civilian use of the invention. However, if the government took title to the invention, the contractor had no assurance of exclusivity. The contractor would then effectively be subject to the threat of a compulsory license in

114. *Id.* at 82 tbl.1.

115. *Id.* at 88.

116. McFetridge reports that with the exception of Merck, 1994 Canadian R&D expenditures as a percentage of worldwide expenditures were less than 2%; e.g. 1.3% for Glaxo, 1.0% for Hoffman LaRoche, 0.7% for Pfizer, 1.2% for Sandoz, 1.4% for Ciba, 1.7% for Eli Lilly, and 6.1% for Merck. *Id.* at 84 n.24.

117. *See* SCHERER, *supra* note 31, at 78-84.

which the government or its potential licensees would have a complete, royalty-free right to use the patent.[118]

From its study of 1,720 contractor inventions, Harbridge House found a substantial difference in contractor utilization of patents depending on whether or not contractors had exclusive rights in civilian markets, although prior commercial experience proved to be the most significant factor.[119] Among contractors with commercial experience, 23.8% who had exclusive rights chose to commercialize their inventions. The figure was only 13.3% among contractors who did not have exclusive rights.[120] Among those without prior experience, there was also a demonstrable difference, although the shares are small—while 6.6% of those with exclusive rights chose to develop the technology, only 2.2% of those without exclusive rights did.[121] In-depth interviews revealed that small firms, new entrants, or firms facing substantial development and technological risks were the most sensitive to the presence or lack of exclusivity. These firms were generally unwilling to invest in commercialization without an assurance of exclusivity.[122] On the other hand, where contractors perceived that they had an advantage in the relevant market or that marginal costs were small relative to potential revenues, development was likely even despite a lack of exclusivity.[123]

The Harbridge study suggests that the relative importance of the markets implicated by a compulsory license matters with respect to innovation. In the case of the "licenses" analyzed, the contractors faced the loss of exclusivity in the civilian sector, which was their primary, most important market. In contrast, the licenses studied by the Eastman Commission implicated the Canadian market, which was viewed as less important by pharmaceutical patent holders. The implication of these two data points is that where the impacted market is important (as in the Harbridge study), an adverse impact on development may be more likely than where the impacted market is unimportant (as in the Eastman study).

In terms of predictability, commercialization was expected, as reported in the Harbridge study, because the government's election to take title to a patent signaled its intent to commercialize that patent in the future. The threat posed by government utilization was thus more similar to the regu-

118. *Id.* at 78-79.
119. *Id.* at 79-81.
120. *Id.* at 80.
121. *Id.*
122. *Id.* at 82.
123. *Id.*

lar licensing regime of Canada in the Eastman Commission study than the sporadic licensing of the U.S. antitrust decrees in the Scherer study.

Thus, the Harbridge licenses were both predictable *and* covered a market significant to the patentee. Although appearing to discourage commercialization, the Harbridge licenses can be distinguished from the compulsory licensing schemes studied by Scherer and the Eastman Commission, where no negative impact on innovation was observed. The Scherer licenses were generally not predictable, issuing as part of investigative probes by the government. Although the Eastman licenses were predictable, they did not cover an important market for the patentees. The implication of these results appears to be that where licenses are unpredictable (Scherer) or implicate insignificant markets (Eastman), there will not necessarily be an adverse impact. However, licenses that are both predictable and affect significant markets, such as the Harbridge licenses, potentially are more risky, and appear to have a greater chance of being accompanied by a negative impact on innovation.

4. Hypothetical Licensing of All Pharmaceutical Inventions

Research conducted by Taylor and Silberston in the form of opinion surveys is consistent with this conclusion. The researchers asked officials from British industries, including the pharmaceutical industry, to predict the impact of a hypothetical system in which all patents, both domestic and foreign, were made available for licensing at reasonable royalties.[124] This extreme form of licensing would be predictable in its reach on future patents and would cover all, and therefore significant, markets. Executives from all industries were asked to evaluate this hypothetical system. The pharmaceutical industry respondents were the most concerned. On average, they predicted that 64% of R&D would be displaced without effective patent protection, as compared to a weighted average of 8% among all industries.[125]

C. Summary of Results

In summary, research to date indicates that, at a minimum, the presence of two factors may be required in order for compulsory licenses to impact innovation. These factors are the predictability of the license being granted and the significance of the market affected by the license. Where either factor is absent, little measurable effect on R&D expenditures has been observed, as shown in the studies performed by Scherer and the Eastman Commission. However when predictable licenses actually (Har-

124. *Id.* at 61.
125. *Id.* at 62.

bridge) or hypothetically (Taylor and Silberston) issue over important markets, the risk of a negative impact is greater. It should be emphasized that although these factors emerged from comparing these studies, other factors such as level of compensation may be just as important. Even if licenses are predictable and affect significant markets, if the price of the license is set at market rates, the license probably will not harm innovation. The factors of predictability and significant market impact may thus be necessary but not sufficient for producing a negative impact on innovation.

V. CASE STUDIES OF INVESTMENT IN INNOVATION AFTER SIX ANTITRUST CONSENT DECREES

To test the hypothesis that only licenses that are both predictable *and* threaten a significant market adversely impact investment in innovation, I studied six cases from the 1980s and 1990s where the FTC issued pharmaceutical compulsory licenses. These cases were the only ones I could find in which licensing, rather than divestiture or other remedies, was prescribed and which were recent enough that data concerning the R&D behavior of the affected firms was available. However, these incidents of licensing are imperfect proxies for compulsory licensing in the international public health sphere for several reasons. The primary objective of these antitrust licenses was to preserve competition, not to increase consumer access to drugs per se. In addition, the licensing events were limited in scope in that they affected specific products produced by specific firms, rather than affecting broad therapeutic areas in entire industries. Such a broad license could be implicated if, for instance, compulsory licenses were made available to all African countries over AIDS vaccines drugs. Nonetheless, the licenses are relevant to the question of whether past compulsory licenses have been accompanied by a decline in innovation.

The licenses I studied were ordered under antitrust consent decrees issued by the FTC. Of the six licenses, four were sporadic and two were predictable, and three covered nascent and therefore relatively less important markets, whereas three jeopardized already developed, and therefore important, markets. Within this modest data set, I considered the relevance of the predictability and market significance of licenses to the R&D outputs of the affected companies. While general trends are reported below, case studies of each FTC order that analyze the license, overall business environment, and subsequent record of innovation by the licensor in the relevant market can be found in the Appendix.

While building on past work, this study introduces several new considerations. First, rather than analyze company-level activity, as did Scherer, I concentrate solely on company activity within an affected therapeutic area. This focus seems appropriate given the size and diversification of pharmaceutical companies—a substantial change to one therapeutic area may not be reflected in the activity of a company as a whole. However, this focus could overstate any impact on net innovation to the extent that a shift in activity away from the affected therapeutic area to another within a company that does not reduce overall R&D would appear as a decline in activity. Second, this study contemplates drug patents from the 1980s and 1990s. Selecting data from this period allowed me to test the robustness of previous findings in light of the trend toward strengthened patent protection, generally and over biological inventions.[126]

A. The Antitrust Drug Licenses

With the exception of the *Eli Lilly* license (see Table 1), all of the licenses I studied arose in the acquisition or merger context.[127] Although each order resulted from negotiations with the FTC, four were "sporadic" in that they occurred only once to remedy a specific concern, and left little discernable expectation of future licenses in the near-term. In contrast, the licenses ordered in the *Eli Lilly* and *Merieux* cases both covered future innovation.[128] In the *Eli Lilly* case, the order called for all patents issued or applied for in the five-year period following the order to be subject to a royalty-free license. In the *Merieux* case, the order required that the acquirer, Institut Merieux S.A. ("Meriuex"), lease Bioscience Connaught's ("Connaught") rabies vaccine business long-term, and that it retain no future interest in the business.[129]

126. *See also* Diamond v. Chakrabarty, 447 U.S. 303 (1980) (expanding patent protection to human made microorganism). *See generally* Jon F. Merz & Nicholas M. Pace, *Trends in Patent Litigation: The Apparent Influence of Strengthened Patents Attributable to the Court of Appeals for the Federal Circuit*, 76 J. PAT. & TRADEMARK OFF. SOC'Y 579 (1994) (noting the increase in judgments finding patents either valid or infringed, as opposed to invalid).

127. *See In re* Ciba-Geigy Ltd., 123 F.T.C. 842 (1997); *In re* Baxter Int'l Inc., 123 F.T.C. 904 (1994); *In re* Dow Chem. Co., 118 F.T.C. 730 (1994); *In re* Roche Holding Ltd., 113 F.T.C. 1086 (1990); *In re* Institut Merieux S.A., 113 F.T.C. 742 (1990); *In re* Eli Lilly & Co., 95 F.T.C. 538 (1980).

128. *See infra* Part VIII.C-D.

129. *See infra* Part VIII.D.

Table 1: Drug License Orders under Antitrust Decrees

Licensor, Invention (Year of order)	Triggering Event	S(poradic) v. G(eneral) license	E(arly) v. M(id) v. L(ate) Stage of Drug Dev't	Nature of Market Affected	Subject of License	Compensation
Baxter, Fibrin Sealant[130] (1997)	Merger	S	M	Mature	Patents +, manufacturing	0
Marion Merrell Dow, Dicyclomine[131] (1994)	Merger	S	L	Mature	Patents +, manufacturing	0
Ciba-Geigy/Chiron, HSV-tk[132] (1997)	Merger	S	E	Nascent	Patents +	"no minimum"
Roche, CD4[133] (1990)	Merger	S	E	Nascent	Patents +	1-3% of net sale
Eli Lilly, Insulin[134] (1980)	Illegal Conspiracy	G	E	Nascent	Future Patents+	Reasonable share of R&D expenses
Connaught, Rabies Vaccine[135] (1990)	Merger	G	L	Mature	Entire Business	Reasonable sum

The stage of development of the affected technology varied among the cases. The *Chiron* and *Roche* cases involved concerns about patents over

130. *In re* Baxter Int'l Inc., 123 F.T.C. 904 (1997).
131. *In re* Dow Chem. Co., 118 F.T.C. 730 (1994).
132. *In re* Ciba-Geigy Ltd., 123 F.T.C. 842 (1997).
133. *In re* Roche Holding Ltd., 113 F.T.C. 1086 (1990).
134. *In re* Eli Lilly & Co., 95 F.T.C. 538 (1980).
135. *In re* Institut Merieux S.A., 113 F.T.C. 742 (1990).

broad basic technologies and therefore covered some early-stage, pre-clinical technologies.[136] Similarly, the *Eli Lilly* license covered patents over insulin produced by novel recombinant DNA methods that had not yet undergone clinical trials at the time the order was issued.[137] The *Baxter* case was prompted by concerns about the merger of two companies that each had products in early development.[138] On the other end of the spectrum, the *Merieux* case involved older patents, and the *Dow* case covered a product market in which generic competition had already been introduced.[139]

The stage of technology is relevant to this analysis because, as described earlier, the drug development process is inherently uncertain. Candidate compounds are eliminated at each step. Taking away patent protection over an early stage technology arguably does not affect a patentee's competitive position as much as a license over a technology that has already surpassed many major milestones. Thus, as reported in Table 1, I characterized licenses over mid-to-late stage technologies as impacting developed and significant markets, and compulsory licenses covering early stage technologies as covering relatively less significant markets.

Importantly, each license involved more than just patents, and most provided for access to know-how and other intangible assets. As stated earlier, this licensing practice reflected the FTC's recognition of substantial market barriers in the drug industry not associated with patents in general, as well as its view that a more robust form of licensing was crucial to the success of licensees.[140] Although individual license orders varied, most contained a provision of either reasonable or no compensation for the rights to use the patented invention. However, the *Baxter* and *Dow* licenses required the manufacturing and delivery of the patented product, so these orders provided for additional compensation to cover the costs of supply.[141]

B. Measurement of the Impact of Drug Licenses

To determine whether licenses brought about a decline in innovation, I looked at patent applications filed by each licensor as reported in the Lexis-Nexis "Utility Patents" database, and where available, considered clinical trial, product launch, and other data specific to the affected com-

136. *See infra* Part VIII.E-F.
137. *See infra* Part VIII.C.
138. *See infra* Part VIII.A.
139. *See infra* Part VIII.B, D.
140. *See supra* note 71 and accompanying text.
141. *See infra* Part VIII.A-B.

pany in the affected product area during the years before and after the ordering of a consent decree. Although several weaknesses were inherent in this approach, as discussed below, patent applications appeared to provide the best means for measuring licensor impact in a specific technology area, which might otherwise be masked by either industry-level or aggregate company data. Although budget information regarding R&D in specific therapeutic areas or interviews with the companies themselves would also have been useful, I was unable to secure either source of information

To identify patent applications, I used keyword searching in the specifications and claims of patent applications that eventually matured into patents. Because queries are sensitive to the search terms used, I selected my terms by reading about the technology area and then formulating searches based on the original patents or patent applications licensed by the FTC order. I also asked a medical doctor to review the terms I used for the more ambiguous technological areas.[142]

To make my analysis less sensitive to the absolute number of patents filed for by the impacted companies during the affected timeframe, I replicated my searches in the entire Utility Patents database. I compared shares of patents filed by an affected company to patents filed for by the general population before, during, and after the affected period so as to eliminate any general bias due to changes in patenting. Based on the normalizations, I saw no difference in the patterns. Because of the time lag between R&D investment and the issuance of a patent based on the investment, I tried wherever possible to capture activity over long pre- and post- licensing event windows. Through this method, and by focusing on patent applications rather than patent grants, I tried to eliminate some of the time lag between innovative activity and patenting. For the older cases, I was able to capture up to fifteen years before and after the license; however, for the most recent cases, I was only able to capture four years of activity after the license.

Although I took the precautions described to filter biases from my data, other factors may affect the accuracy of my results. For example, companies may choose not to patent or to delay patenting inventions for strategic or other reasons. This fact tends to discredit the use of patenting activity as a measure of company investment in innovation. However, the patents at issue in the six cases at hand were most likely important to the relevant companies because the FTC considered the patents important enough to require that they be licensed. Another limitation is the possibility that the companies shifted their intellectual protection strategies to-

142. The chosen search terms are described in the case studies in the Appendix.

wards trade secrecy, thereby maintaining their pre-licensing level of R&D while reducing patent output. If this is the case, post-licensing investment in innovation will have been understated by the patent counts.

To address the problems presented by using patents as a measure of investment in innovation, I used other measures of company commitment to each therapeutic area. I searched BioSpace Inc.'s Clinical Competitive Intelligence System for clinical trials that had been in progress sometime in the 2000 to April 2002 period.[143] The BioSpace database covers about 50% to 60% of all private and public clinical trials, and is reportedly the most comprehensive of all clinical trials database, including the development database offered on the Pharmaceutical Research and Manufacturers of America website. I also looked at each company's annual reports and websites for new drug announcements, infrastructure commitments, and other clues about each firm's commitment to innovation in the affected area.

The main limitation of this study is that it comprises only six data points and therefore cannot support any statistical conclusions. At most, the case studies analyzed in this Article provide anecdotal illustrations of how compulsory licensing might impact investment in innovation.

C. Impact of Compulsory Licensing

1. Sporadic Licensing

Based on patent application activity (see Figure 1) and both qualitative and clinical trial evidence (see Appendix), it appears that none of the four "sporadic" licenses were accompanied by a reduction in innovation. This is in line with both the existing literature and common-sense expectations; the element of surprise and the unpredictable nature of the licenses presumably made it impossible for any of the licensors to change their behavior in anticipation of the license.

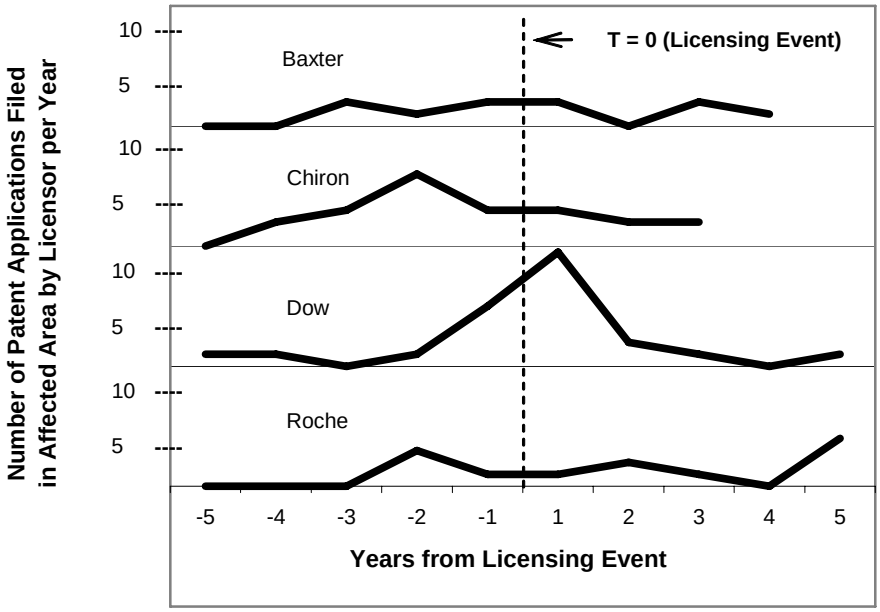
For each licensing event, Figure 1 shows the absolute number of patents in the therapeutic area affected by the license filed by a licensor in the years preceding and following the FTC order. For the most part, I counted applications filed in twelve-month increments beginning with the month following the order, rather than based on the calendar year.[144] In the in-

143. *See generally* BioSpace: Competitive Clinical Intelligence System, (Biospace 2003) *at* http://www.biospace/com/ccis/index.cfm (providing a searchable database of, *inter alia*, clinical trials).

144. For the last two years of the Baxter data, I used international patent filing data, which captures all applications that have been on file for at least eighteen months, to supplement U.S. filing data given the long lags between filing and issue of fibrin sealant pat-

stances of Baxter International ("Baxter") and Roche Holding Ltd. ("Roche"), there appeared to be no interruption of the general trend of patent applications. With Chiron Corporation ("Chiron"), the absolute number of patent applications peaked before the licensing order, but the company continued to steadily file applications in successive years. The opposite is true for Merion Merrell Dow ("Dow"), where the twelve-month period following the order was the most productive in terms of the number of applications filed. Based on the few data points provided, no systematic negative impact on patent applications was observed. This result is in line with earlier research.

Figure 1: Sporadic Licenses - Absolute Patenting



Although the graphs do not reveal clear trends, compulsory licensing did not cause dramatic reductions in R&D according to measures besides patent counts. In the instance of Baxter, marketing considerations seemed to encourage the firm to continue investing in its fibrin sealant product line. After several years of competition with Haemacure Corporation ("Haemacure"), its licensee, Baxter still retained a market share of 75% and enjoyed a high revenue growth rate, particularly with respect to its

---

ents. As a result I relied on calendar twelve-month increments in order to capture as much application activity as possible.

other blood products.[145] With Chiron and Roche, each company currently captures a considerable share of clinical trials, signaling long-term commitments to the affected product lines. As for Dow, the dwindling importance of dicylomine as a treatment for irritable bowel syndrome ("IBS") makes it probable that factors other than the license influenced the company's decisionmaking. Each of these examples is explored more fully in the Appendix.

2. Predictable Licensing

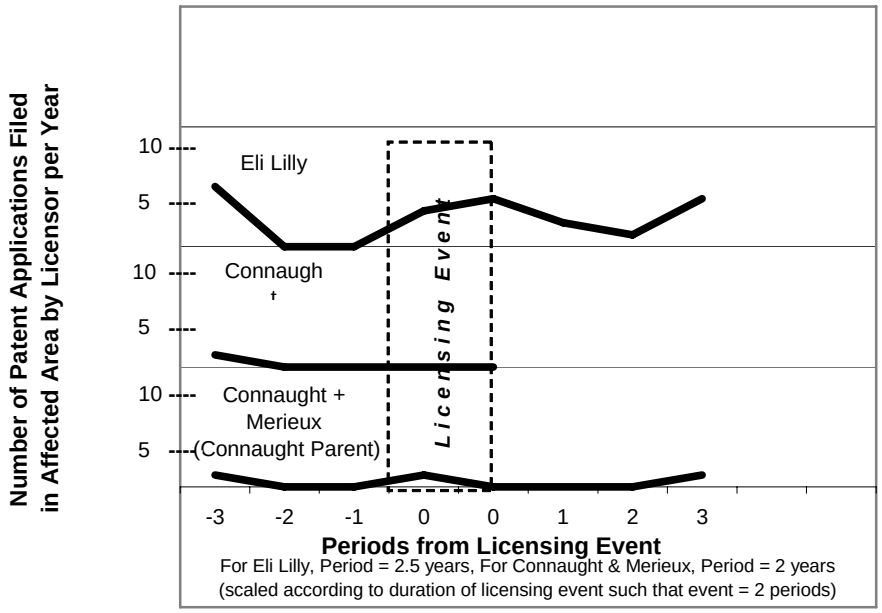
The two instances of predictable licensing present a more complex problem. While both Eli Lilly and Connaught/Merieux were subject to licenses covering future innovation, Eli Lilly flourished during the time of its compulsory license while Connaught claimed to be adversely impacted. This difference is reflected in Figure 2, which shows the absolute patent filings of Eli Lilly and Connaught before, during, and after the compulsory licensing period.

In the Eli Lilly example, the data indicate that the licensing event was not coupled with a negative change in the company's patenting activity. Innovative outputs actually rose rather than declined. In the Connaught example, patent application counts are of limited value because there was very little patenting activity in the relevant therapeutic area. Although Connaught did not file any patents during the four years it was affected by a licensing agreement, it also did not file any patents prior to the licensing. However, evidence other than patenting suggests that Connaught's inventive activities declined after licensing. For example, Connaught reported to the FTC that the license prevented it from upgrading its facilities.[146] Also, Merieux's continued patenting activity before, during and after the licensing (see Figure 2), suggest that Merieux, which was not subject to the license continued to innovate even while Connaught did not. A more detailed discussion of these two case studies follows.

145. *See infra* Part VIII.A.

146. *In re* Institut Merieux S.A., 113 F.T.C. 742 (1990).

Figure 2: Predictable Licenses - Absolute Patenting



The consent decree in *Eli Lilly* was very broad. It provided access to Eli Lilly's intangible assets for all who, within five years of the decree, stated a bona fide intention to produce and sell insulin products in the United States. Included in the intangible assets made available by the decree were all patents issued to and applied for by Eli Lilly during the five-year period.[147] One limitation on the broad decree was a provision requiring that a licensee contribute to Lilly's R&D expenses if asked to do so.[148] Because the order was so broad, providing for an unlimited amount of licensing covering both extant and future patents on any insulin technology, it effectively prevented Lilly from exercising its patent rights over insulin technology during the affected period. Faced with this severe version of compulsory licensing, one might expect Lilly to have been discouraged from further developing its insulin product for the five-year period set forth in the order, or perhaps to have delayed patent applications until after the period had expired, relying on trade secrets or other forms of protection in the interim.

However, Eli Lilly continued to dominate the emerging human insulin market in performing R&D, surpassing major milestones during the period from 1980 to 1985 covered by the consent decree. Following the initial

147. *In re* Eli Lilly & Co., 95 F.T.C. 538, 1980 FTC LEXIS 85, *17 (1980).
148. *Id.*

production of human insulin through recombinant DNA techniques in 1978, Lilly initiated clinical trials of its human insulin product, "Humalin," in the United States in 1980, and invested in additional research facilities.[149] In 1982, Lilly was rewarded for its efforts, receiving the first FDA approval for human insulin in the United States.[150] Eli Lilly was actually more active in filing for patents during the five-year period of the decree than it was during the previous and subsequent five years combined.

Several factors seem to have motivated Eli Lilly's continued innovation during this period. First, and perhaps most importantly, Lilly was extremely well-positioned to exploit and benefit over the long-term from the genetics revolution emerging at the time. The company maintained its early lead into the testing and commercialization phases of insulin, and over the decade following expiration of the order was usually first or second to introduce products of increasing purity on the market.[151] In addition, Lilly historically enjoyed a position of market leadership. As it stated in the 1984 Annual Report: "With our historical position in diabetes, and the patients we serve, it is clear we have to aggressively go out and look at proinsulin. If it is potentially better, then we have an obligation to bring it forward. We owe this to society and humanity."[152]

Furthermore, insulin has long been one of Eli Lilly's most important products. Shortly after Lilly took the first license to insulin in 1923, insulin accounted for half of the company's profits, and it was the company's second largest revenue producer in 1994.[153] Finally, Lilly has faced continuous pressure from its main competitor, Novo Nordisk. In 1980 the two companies together controlled 77% of the insulin market–53% by Eli Lilly and 24% by Novo Nordisk. By 1995, the figure rose to over 90%, with Eli

149. *See* ELI LILLY, 1981 ANNUAL REPORT 5-6 (1982) [hereinafter ELI LILLY 1981 ANNUAL REPORT].

150. *See, e.g., A Market Face-off for Two Insulin Pioneers,* BUS. WK., Nov. 1, 1982.

151. *See, e.g.*, CLAYTON M. CHRISTENSEN, ELI LILLY AND COMPANY: INNOVATION IN DIABETES CARE 4-5 (Harv. Bus. Sch., Case Study no. 9-696-077, 1996).

152. *See* ELI LILLY, 1984 ANNUAL REPORT 17 (1985) [hereinafter ELI LILLY 1985 ANNUAL REPORT]. Eli Lilly's position of market leadership began in 1923, with its exclusive license over the manufacture of insulin with the University of Toronto, where Nobel Prize Winner Frederick Banting did his ground-breaking work. *See* Irving S. Johnson, *Human Insulin from Recombinant DNA Technology*, 219 SCIENCE 632 (1983).

153. *See* CHRISTENSEN, *supra* note 151, at 1, 3. Insulin has continued to be a high revenue generator, despite being viewed as a commodity product because of significant barriers to entry including the high cost of clinical trials for new biotechnology products and the cost of efficient manufacturing facilities. *See id.* at 4.

Lilly capturing 46% and Novo Nordisk capturing 45% of the market.[154] The pressures generated by market leadership, a desire for market dominance, and competition provided Lilly significant motivations to keep innovating, notwithstanding the temporary suspension of patent rewards.

The case study of Connaught's business also involves predictable licensing. At the time it received the FTC order, Merieux was the sole supplier of rabies vaccines in the United States. Prior to the order, Merieux had acquired the company Connaught, one of two potential entrants into the market.[155] Worried that Merieux's monopoly would remain unchallenged, the Commission called upon Merieux to lease Connaught's entire rabies vaccine manufacturing business, including both tangibles and intangibles, to an approved lessee for a minimum of twenty-five years.[156] However, Merieux was unable to find a suitable buyer for Connaught's manufacturing business.[157] Nearly four years after the decree had issued, the FTC withdrew the leasing requirement from the order.[158]

The requirement that Merieux lease Connaught presumably reduced Merieux's incentive to invest in Connaught's facilities. Merieux stated as much in its request to the FTC that the leasing requirement be dropped. The company claimed that "the continuing lease requirement may be harmful to competition . . . because it adversely affects Connaught's ability to respond to the increased demand for vaccine with capital investments to upgrade and expand the business's productive capacity."[159] Although evidence of this decline was not provided in the consent order, Connaught did not file any patents for rabies vaccine inventions during the contested period. In contrast, Merieux (which ultimately became Aventis) filed five such patents in the subsequent years.

One possible reason that Connaught temporarily discontinued patenting is its potential entrance in the U.S. market, over which Merieux had a stronghold. In this light Merieux may have viewed any enrichment of Connaught's business as tantamount to enriching a potential competitor in the same market. Even though the consent decree was flexible enough to enable Merieux to recoup any improvements it made to the Connaught business, given that the decree called for a reasonable lump sum payment by the licensee, Merieux's competitive interests arguably created an incen-

154. *Id.* at 17 exh.9.

155. *In re* Institut Merieux S.A., 113 F.T.C. 742, 1990 FTC LEXIS 291, *3-4 (1990).

156. *Id.* at 7-9.

157. *In re* Institut Merieux S.A., 117 F.T.C. 473, 474-75 (1994) (modifying 1990 order).

158. *Id.* at 482.

159. *Id.* at 477.

tive to neglect Connaught's rabies vaccine business while enriching its own. Indeed, during the same period in which Connaught did not file for any patents, Merieux sustained its lead in the rabies vaccine business, filing for a patent in late 1991, and launching a new product, Raboral, in 1992.[160]

D. Results

These results, although limited, lend support to the theory that only drug licenses that issue predictably in significant markets are likely to harm innovation. Of the six companies subjected to compulsory licensing, Merieux was the only one that exhibited a decline in patenting. Merieux's licensing event was the only one that was both anticipated and affected a market that was significant to the company. Although the data used in this study cannot prove that the licensing event caused Merieux's decline in patenting, it does indicate how pharmaceutical companies might react to these types of compulsory licenses.

Table 2: Summary of Antitrust Case Results

Antitrust Licenses	Sporadic v. General License	Nature of Market Affected	Perceived or Actual Negative Impact?
Baxter	Sporadic	Developed	No
Dow, Roche	Sporadic	Developed	No
Chiron/Ciba-Geigy	Sporadic	Nascent	No
Roche	Sporadic	Nascent	No
Eli Lilly	General	Nascent	No
Merieux/Connaught	General	Developed	Yes

The results of this study are contrary to the prevalent assumption that compulsory licensing categorically harms innovation. Were the assumption true, all six cases would reveal a drop in investment in innovation subsequent to licensing, yet no such uniform downward trend was ob-

160. *See Merieux Doubles Profits, Sees Growth in Rabies Vaccine*, AGENCE-FRANCE-PRESSE, Mar. 16, 1992 [hereinafter *Merieux Doubles Profits*], *available at* 1992 WL 8462395.

served. In fact, the opposite seems to be true—in all cases but one, activities of innovation continued at the same or even higher pace than before the advent of a license. These results cast doubt on concerns that compulsory licensing is uniformly deleterious.

The study also suggests that, notwithstanding the absence of a uniform downward trend, the circumstances surrounding a compulsory licensing event can impact innovation. Where a license is predictable and the market it affects is significant, a negative impact on innovation may be possible. More caution may be in order when such licenses are contemplated over patents held by companies or individuals who depend on patent profits.

VI. IMPLICATIONS FOR DRUG LICENSING IN DEVELOPING COUNTRIES

As discussed in the preceding section, at least two factors may influence whether compulsory licenses impact pharmaceutical innovation. These factors, namely the predictability of the license and the significance of the affected market, have implications for the compulsory licensing of drugs by developing countries.

An important consideration in determining whether compulsory licenses taken by developing countries will impact innovation is the type of drug licensed. Developing countries care about two categories of drugs, each with its own set of incentives.[161] First, there are "global" drugs that are created for rich markets, but are also useful in developing countries. Examples of these are cancer drugs and AIDS therapeutics.[162] Second, there are drugs specific to developing countries. Examples of these include drugs to treat malaria or tuberculosis, or an AIDS vaccine specific to strains of the virus found primarily in Africa.[163] Historically, such drugs have not been the priority of pharmaceutical companies. For example, a 2001 Harvard School of Public Health survey of twenty large pharmaceutical firms found that "[o]f 11 responders, eight had done no research over the past year in tuberculosis, malaria, African sleeping sickness, leishmaniasis, or Chagas disease; seven spent less than 1% of their research and development budget on any of these disorders."[164]

Funds for researching diseases specific to developing countries often come from public or philanthropic resources such as the Centers for Dis-

161. *See* LANJOUW, *supra* note 91.

162. *See id.*

163. *See id.*

164. Ricki Lewis, *Fighting the 10/90 Gap*, SCIENTIST, May 13, 2002, http://www.the-scientist.com/yr2002/may/lewis_p22_020513.html (last visited July 22, 2003).

ease Control or public-private partnerships like those created by the International AIDS Vaccine Initiative. The Medicines for Malaria Venture, for instance, matches academic researchers with private firms to generate collaborations in malaria medicines, an area that has largely been overlooked by industry.[165] The Global Alliance for Tuberculosis Drug Development, partly sponsored by the Rockefeller Foundation, similarly tries to shift product development risk away from drug companies by conducting costly clinical trials for promising drug candidates.[166] Efforts to develop an AIDS vaccine for countries in Africa have likewise been collaborative.[167]

Research to date suggests that if compulsory licenses are taken in less significant markets, their impact on innovation should be marginal. For global drugs such as AIDS therapy, this would imply that compulsory licenses that are limited to developing countries (i.e. ancillary markets) and do not impact the target markets for the drugs (i.e., rich countries) might not be detrimental to research efforts in the rich developed countries. This is in accord with common sense. For global drugs, companies are responsive to the incentives provided by wealthy markets and consumers. If these incentives stay intact, selective compulsory licensing for developing nations should have little impact on overall R&D investment as long as the affected market is limited to developing countries.

On August 30, 2003, a historic accord on compulsory licensing was announced addressing this concern. After several days of negotiations, the United States and other WTO countries effectively agreed to allow poor countries to import generic drugs through compulsory licenses as long as measures to prevent re-exportation of the drugs to other, rich markets are taken.[168] For example, such measures include special packaging or coloring to clearly delineate drugs that have been exported under compulsory

---

165. Martin Enserink *Malaria Researchers Wait for Industry to Join the Fight*, 287 SCI. 1956, 1958 (2000).

166. *Exotic Pursuits*, ECONOMIST, Jan. 30, 2003, *available at* 2003 WL 6244875.

167. *See, e.g.*, Alexandra Bojak et al., *The Past, Present, and Future of HIV-Vaccine Development: A Critical View*, 7 DRUG DISCOVERY TODAY 36, 41-43 (2002) (describing the funding of basic research by the European Union and other governments and the continued need for collaboration between rich and poor countries and for money from donor organizations such as the European Vaccine Efforts); Paul J. Weidle, et al., *HIV/AIDS Treatment and HIV Vaccines for Africa*, 359 LANCET 2265 (2002) (describing HIV vaccine trials in Africa as sponsored by the NIH, CDC, IAVI, and other public and philanthropic organizations).

168. *See, e.g.*, WTO, The General Council Chairperson's Statement, Aug. 30, 2003 [hereinafter WTO Aug. 30 Statement], *at* http://www.wto.org/english/news_e/news03_e/trips_stat_28aug03_e.htm (last visited Sept. 6, 2003); Becker, *supra* note 87, § 1, at 14.

licenses from drugs sold in rich countries.[169] The United States has demanded that the scope of the accord cover life-threatening diseases.[170] While some details about its coverage are yet to be resolved,[171] the accord is indisputably intended to reach AIDS therapy drugs.

The implication is somewhat different for drugs developed to treat diseases endemic to developing countries, such as malaria. As discussed above, much of the research on these diseases is carried out or facilitated by public or philanthropic institutions, for whom patent protection and the promise of a patent monopoly are less, if at all, important. In addition, the potential for monopoly abuse which compulsory licenses are designed to counter could also be less likely. If pharmaceutical companies, on the other hand, begin investing significantly in such disease areas due to the introduction of patent protection, as is hoped, a compulsory license covering all developing country markets might well usurp the primary target markets. Threatening or implementing licenses on a regular, predictable fashion may deter pharmaceuticals from initiating and carrying out R&D investments.

Based on these observations, and focusing exclusively on innovation concerns, one can make a preliminary case for employing different approaches to compulsory licensing depending on whether global or developing country-specific drugs are licensed. Because the relative importance of developing country markets is small when it comes to global drugs, the incentive to develop these drugs, which comes from the developed world, is not substantially impacted. This means that allowing developing countries to take compulsory licenses to AIDS therapy drugs should not produce a negative impact on AIDS therapy research and development. The recent WTO accord is entirely appropriate in this regard.

The picture is different when it comes to drugs being developed specifically to treat developing country diseases, such as AIDS strains endemic to Africa. Compulsory licenses for developing countries could cover the entire target market of local and international pharmaceuticals. The threat of systematic compulsory licensing of these drugs may make a difference and could cause some companies to avoid these markets altogether. To the extent that the compulsory licensing framework that devel-

169. WTO Aug. 30 Statement, *supra* note 168.

170. Becker, *supra* note 87, § 1, at 14.

171. Editorial, WTO Takes a First Step, 362 LANCET 753 (Sept. 6, 2003) (arguing for an interpretation of the agreement broader than including only drugs to treat HIV/AIDS, tuberculosis, and malaria), *available at* http://pdf.thelancet.com/pdfdownload?uid=llan.362.9386.editorial_and_review.27086.1&x=x.pdf.

ops under the WTO accord also covers such diseases, as it likely will,[172] special care should be taken to ensure that incentives remain intact. To date, the patent incentive has arguably not successfully prompted R&D in these medicines. Therefore, the importance of preserving the current patent incentive should not be overstated. This is particularly true because of the strong role played in this area by public and philanthropic institutions, which presumably are not motivated by monopoly profits.

Compulsory licensing is far from an easy solution; exploiting it fully requires political will and technical capability. In the past, countries that have elected to take licenses have had to endure lawsuits, pressure, and threats of trade sanctions from the United States.[173] In addition, producing drugs pursuant to a license requires a level of technical and manufacturing capability possessed by few countries.[174] The August 2003 WTO accord significantly deals with these issues. Still, meeting the accord's requirements for licensing could prove challenging, or at least bureaucratic.[175] Over-reliance on compulsory licensing may also produce unintended negative downstream impacts on society.

While high drug prices comprise only one aspect of the AIDS problem,[176] the WTO accord evidences the growing realization that increasing access to drugs must be a part of the solution. This is partly due to a number of factors that have shifted attention towards affordable treatment and vaccination rather than prevention alone.[177] The initial push for prevention

---

172. *See id.*

173. The U.S. and western pharmaceutical companies have routinely used the Special 301 mechanism for authorizing trade sanctions and lawsuits at the WTO and in domestic courts to oppose policies implemented by other countries that are unfavorable to pharmaceutical company interests. *See, e.g.*, Sarah Boseley, *How the U.S. Wields a Big Stick for Big Pharm*, GUARDIAN, Feb. 18, 2003 (describing actions against Thailand); Carin Håkansta, *The Battle on Patents and AIDS Treatment*, 16 BIOTECH. AND DEV. MONITOR 34 (1998) (describing early battles against India in the TRIPS court), *available at* http://www.biotech-monitor.nl/3406.htm (last visited Aug. 27 2003).

174. *See* Attaran & Gillespie-White, *supra* note 5 (describing non-patent barriers to drugs, such as insufficient finances, lack of political will, poor medical care and infrastructure, inefficient drug regulatory procedures, and high tariffs and sales taxes).

175. Becker, *supra* note 87, § 1, at 14 (describing the concerns of some groups that "red tape" will discourage use of compulsory licenses).

176. Some have suggested that cheap drugs might actually aggravate the problem by diverting attention away from prevention. *See, e.g.*, Michael Specter, *India's Plague*, NEW YORKER, Dec. 17, 2001, at 74.

177. *See, e.g.*, *Hope for the Best. Prepare for the Worst—the Future of Aids.*, ECONOMIST, July 11, 2002 (describing the growing intensity in AIDS vaccine research in light of the limitations of prevention and treatment), *available at* 2002 WL 7246756; Michael Specter, *The Vaccine*, NEW YORKER, Feb. 3, 2003, at 54.

was based on the conventional wisdom that prevention (through education, the empowerment of women, and distribution of condoms) is the best cure for the AIDS problem, and that AIDS therapy regimes were too expensive and complicated to be suitable for developing countries. However, in the past two years, experience has shown that people in developing countries can and will comply with drug regimes at levels equal to or greater than their Western counterparts. At the same time, there has been a realization that attitudes and culture are hard to change and that solutions other than behavioral transformation must be explored.[178] In addition, the availability of drugs is crucial not only for treating sick patients but also for diagnosing and stopping the spread of AIDS because "people who are infected and cannot be treated have little incentive to get tested; that, in turn, means they do not know they are infected, and so do not take precautions against infecting others."[179] All of these factors have made access to AIDS drugs a more pressing and realistic objective.[180]

Still, the focus on cheap drugs for therapy today should not draw attention away from the hope of an AIDS vaccine tomorrow. How compulsory licensing programs are designed and implemented matter in this regard, and the emerging regime of compulsory licensing deserves continued attention in this respect.

VII. CONCLUSION

Although modest, the data analyzed in this study yield potentially surprising implications for the current debate over compulsory licensing. At a minimum, they challenge the wholesale rejection of licensing schemes for AIDS drugs based on their perceived negative impact on

178. *See* Michael Grunwald, *All-Out Effort Fails to Halt AIDS Spread; Botswana's Program Makes Progress, But Old Attitudes Persist*, WASH. POST, Dec. 2, 2002, at A1; Rosenberg, *supra* note 7.

179. *Hope for the Best. Prepare for the Worst—the Future of Aids*, *supra* note 177.

180. Even before the August 2003 WTO accord, the pharmaceutical industry voluntarily reduced prices on a number drugs in recognition of the humanitarian crisis. *See, e.g.*, Geoff Dyer, *How Do You Price AIDS Treatment?*, FIN. TIMES, Mar. 26, 2003, at 13 (describing Roche's statement that it will not enforce intellectual property rights on its AIDS drug Fuzeon, priced at $20,000 a year per user, in sub-Saharan Africa); Grunwald, *supra* note 178, at A1 (describing Merck's offer of an unlimited supply of antiretroviral drugs to Botswana); Paul Jacobs, *Gilead Unveils AIDS Drug Plan*, SAN JOSE MERCURY NEWS, Apr. 4, 2003 (describing how Gilead Sciences plans to offer its successful AIDS drug Viread to 68 developing countries at substantially reduced prices), *available at* 2003 WL 14985084; *see also* Geoff Dyer, *Investors Warn Drugs Industry of Backlash over Health Crises*, FIN. TIMES, Mar. 24, 2003, at 25 (describing investor pressure for price cuts).

AIDS innovation. They also invite consideration of how compulsory licenses are designed and implemented. They suggest that, based on innovation concerns, the use of different kinds of licenses over global and developing country diseases may be appropriate given the different incentives driving innovation in these areas.

VIII. APPENDIX: ANTITRUST LICENSE CASE STUDIES

A. Baxter/Fibrin Sealant

1. The Order

In early 1997, the FTC ordered Baxter to license its rights to fibrin sealant, a topical agent used to control surgical bleeding, in connection with Baxter's acquisition of Immuno International AG ("Immuno").[181] Although the product had been available in Europe for several years before the order, Baxter and Immuno were two of just a handful of companies seeking FDA approval for the first product launch in the U.S. market,[182] estimated shortly after the order to be worth up to $200 million annually.[183]

The part of the order pertaining to fibrin sealant required Baxter to provide a license to all of Immuno's intangible assets and rights (including patents, trade secrets, technology, know-how, specifications, customer lists, and FDA approval data) related to the R&D, manufacture, and sale of fibrin sealant.[184] The order mandated one commission-approved licensee.[185] Once Baxter obtained FDA approval, the order required the company to supply the licensee with Immuno's fibrin sealant product until the licensee received approval for its own product.[186] In exchange, the order required the licensee to reimburse Baxter for the costs of manufacturing the fibrin sealant product while demonstrating a continuing commitment to obtain approval from the FDA for its own fibrin sealant product.[187] Other portions of the order called for the divestiture of Immuno's Factor VIII assets.[188]

---

181. *In re* Baxter Int'l Inc., 123 F.T.C. 904 (1997).
182. *Id.* at 906.
183. *See* Gary Shepherd, *To Haemacure, 'Scab' is Not a Four-Letter Word,* TAMPA BAY BUS. J., Sept. 11, 1998, *available at* 1998 WL 33483931.
184. *Baxter*, 123 F.T.C. at 910, 921.
185. *Id.* at 921.
186. *Id.*
187. *Id.*
188. *Id.* at 910-916.

Within six months of the order, the FTC approved Haemacure as the fibrin sealant licensee.[189] A little over a year after the order was issued, in May 1998, Immuno's fibrin sealant received FDA approval, and both Baxter and Haemacure introduced the product into the U.S. market.[190] Over the next few years, Baxter and Haemacure were the only sellers of fibrin sealant in the U.S. market, with Baxter capturing 75% of the market in 1999.[191] The FTC approved several requests by licensee Haemacure to extend the license, and in 2002, Haemacure estimated that the license could expire in 2004.[192]

2. Impact on Innovation

Baxter's interest in pursuing follow-on innovation and products could have hypothetically declined with their loss of exclusive control over the market because the license required them to share late-stage technology and profits with Haemacure. On the other hand, the late stage of the technology possibly reduced other uncertainties associated with the technology, and the license potentially provided the chance to capture additional revenue with little investment.

After the order, Baxter continued to invest in fibrin sealant and related therapeutic areas. This is shown by their patenting activity, new product development, and clinical trials. The company filed about as many patent applications for this technology in the five years following the order as in all years prior to it.[193] Additionally, Baxter introduced a follow-on application device,[194] and worked on a patch, rather than liquid, version of the product.[195] Also, the company conducted clinical trials on a hemostatic

189. *See For Your Information*, Fed. Trade Comm'n Office of Public Affairs, Aug. 1, 1997, *at* http://www3.ftc.gov/opa/1997/08/petapp40.htm (last visited Aug. 11, 2003).

190. *See* Christiane Truelove, *Baxter's Bloodline*, MED. AD NEWS, Sept. 1, 1999, *available at* 1999 WL 12977876; *Haemacure Announces Fiscal Year 2001 Financial Results*, CAN. NEWSWIRE, Jan. 11, 2002, *at* http://www.newswire.ca/releases/January 2002/11/c1986.html (last visited Aug. 11, 2003).

191. *See* HAEMACURE CORP., 1999 ANNUAL INFORMATION FORM 8 (2000), http://www.haemacure.com/pdf/infoform/Ai280400a.pdf (last visited Aug. 11, 2003).

192. *See Haemacure Announces Fiscal Year 2001 Financial Results*, *supra* note 190.

193. This finding is based on a date and assignee search of the LEXIS patent application database using the keyword "fibrin sealant." The company successfully obtained six patents prior to the order, and obtained five patents after it.

194. *See* News Release, Baxter, Baxter's New Fibrin Sealant Application System Cleared by FDA (July 10, 2000), *available at* http://www.baxter.com/utilities/news/releases/2000/07-10tissomat.html (last visited Aug. 11, 2003).

195. *See* Glenn M. Reicin & Jason H. Wittes, *A Feel-Good Analyst Meeting*, Morgan Stanley Dean Witter, Mar. 23, 2001, at 8 (on file with author).

sealant, which it subsequently introduced on the market.[196] In 2000, the company announced a $400 million commitment to upgrade facilities used for fibrin sealant and other plasma and recombinant DNA products.[197] Overall, Baxter did not appear to reduce its investment in R&D in fibrin sealant and related products.

Product economics may explain Baxter's interest and aggressive marketing concerning fibrin sealant. According to a Lehman Brothers report issued in late 1999, the projected revenue compounded annual growth rate for fibrin sealants was over 35%, which was the highest rate in Baxter's blood product division.[198] Additionally, Baxter was projected to capture nearly 60% of the international fibrin sealant market by 2001, of which approximately half was estimated to come from the United States.[199] Other companies, including Aventis, Omrix, the American Red Cross, Vitex, and a Bristol-Meyers Squibb subsidiary also developed fibrin sealants.[200] Thus, Baxter was plausibly motivated to capture the first-mover advantage in the years just after the license was ordered.

B. Marion Merrell Dow/Dicyclomine

1. The Order

In late 1994, the FTC ordered Dow to license its rights to dicyclomine, a product used for the treatment of IBS.[201] At the time of the order, Dow's product was already on the market with only 60% of the $7 to $8 million market, due to generic competition.[202] Dow's acquisition of Rugby Darby, the only generic company approved to manufacture the drug at the time, raised antitrust concerns.[203]

Given that Rugby Darby already made dicyclomine, some key patents were presumably expired, but other barriers, described by the FTC order as "difficult and time consuming," prevented other generic companies from entry.[204] Accordingly, the order required Dow to provide a per-

196. According to Biospace's CCIS database (based on date search and keyword "sealant").

197. *See supra* note 196.

198. *See* David A. Gruber et al., *A Potential Source of Stability*, Lehman Brothers, Oct. 6, 1999 (on file with author); Reicin & Wittes, *supra* note 195, at 14.

199. *See* Reicin & Wittes, *supra* note 195, at 14.

200. *See* HAEMACURE CORP., *supra* note 191, at 8.

201. *In re* Dow Chem. Co., 118 F.T.C. 730, 736-38 (1994).

202. *See Lannett Expects Increased Sales and Profit with the Launch of its Third and Most Significant Generic Drug Product*, BUS. WIRE, July 21, 1994.

203. *Dow*, 118 F.T.C. at 732-33.

204. *Id.* at 732.

petual license to a commission-approved licensee, including all formulations, patents, trade secrets, technology, know-how, and specifications.[205] The order did not specify a price, but stated that there was "no minimum price" for the license, implying that no potential deal could be rejected on the basis of price. The order also required Dow to provide manufactured dicyclomine to the licensee until it received FDA approval. In exchange, the order mandated that the licensee pay up to 48% of the wholesale price of the dicyclomine, while attempting to obtain FDA approval for its own manufacturing facilities.

2. Subsequent Developments

Within one year of the order, Hoechst Marion Roussel, Inc. ("HMRI"), Dow's successor through merger, requested and obtained FTC approval to award a license to Endo Laboratories, a subsidiary of Dupont Merck Pharmaceutical Company.[206] During this time, other generic companies entered the dicyclomine market,[207] causing the IBS market to mature by the last half of the 1990s, with few new product introductions until 2000.[208] Although dicyclomine was one of just three main products in the anti-cholinergic and anti-spasmodic segment of IBS medications, other medication segments such as anti-diarrhea and constipation were more important.[209] Dicyclomine's share of the overall IBS medication market eventually dwindled to less than 2% in 2000.[210]

3. Impact on Innovation

Even though generic manufacturers were producing Dicyclomine at the time of the order, the license conferred advantages principally associated with the head start that Dow achieved over the generic manufacturers. It is unclear whether much opportunity existed for innovation in this particular therapeutic area, because the product was already mature. Still, assuming that Dow and its successor HMRI had to make a decision about the IBS market, its weak market position and the relatively small size of the dicyclomine market could potentially deter any future investment.

---

205. *Id.* at 736.

206. *See For Your Information*, Fed. Trade Comm'n Office of Public Affairs, July 19, 1996, http://www3.ftc.gov/opa/1996/07/petapp41.htm (last visited Aug. 11, 2003).

207. *Id.*

208. *See* Stewart Adkins et al., *Irritable Bowel Syndrome, Poetry in Motion*, Lehman Brothers, Sept. 2, 1999, at 19 (on file with author).

209. *See id.* at 6.

210. *See* Jeffrey Chaffkin et al., *Company & Therapeutic Prescription Statistical Update*, Paine Webber, Oct. 23, 2000, at 96 (on file with author).

A year after the license issued, HMRI stopped filing for patents.[211] However, it is difficult to attribute this absence in activity only to the license, because the year following the license was the most productive year in terms of number of patent applications, with six patent applications filed. Although it is possible that these were merely the result of pre-license innovation activities, the presence of other factors such as dwindling market share and the earlier loss of patent protection could each plausibly explain the rise and then discontinuation of patenting. Even though little can be definitively concluded about this case, it does not appear that licensing alone entirely explains HMRI's exit from the R&D IBS market.

C. Eli Lilly/Insulin

1. The Order

In 1980, the FTC charged Eli Lilly with involvement in a wide-ranging conspiracy, dating back to 1952, with other manufacturers of pancreatic insulin.[212] The FTC ordered the firm to license the know-how and rights relating to both its existing and future insulin-related patents.[213] Any potential entrant who, within five years of the decree, stated a bona fide intention to produce and sell insulin products in the United States would obtain access to Lilly's intangible assets, including all patents issued and applied for during the five-year period.[214] Significantly, Lilly could impose a charge on the licensee equal to a "[r]easonable pro rata share of the amounts actually spent by Lilly in acquiring, or financing the research and development . . . [of] such licensed patents and know-how," in addition to a requirement to give grantbacks.[215] The order also required licensees to keep all production in the United States.[216]

2. Subsequent Developments

No information is available on whether any companies came forward and took advantage of the compulsory license made available by the

---

211. While other companies have continued to develop IBS medications, with sixteen products in clinical trials during the 2000-2002 period according to Biospace, Dow/HMRI has not participated in any reported drug development activities. Search conducted by the author of the Biospace database using keywords "irritable bowel syndrome" or "dicyclomine."

212. *In re* Eli Lilly & Co., 95 F.T.C. 538, 1980 FTC LEXIS 85, *5 (1980).

213. *Id.* at *17, *23.

214. *Id.* at *17.

215. *Id.* at *24.

216. *Id.* at *23.

consent decree.[217] However, Lilly continued to dominate the emerging human insulin market in both research and development, surpassing major milestones during the five-year period covered by the consent decree. In 1980, following the initial production of human insulin through recombinant DNA techniques in 1978, Lilly initiated clinical trials in the United States of its human insulin product "Humalin" and invested in research facilities to carry out additional work.[218] In 1982, the FDA rewarded Lilly for its efforts with the first approval for human insulin in the United States.[219]

3. Impact on Innovation

The broad order, covering future patents issued on any insulin technology and allowing a potentially large number of licensees, effectively prevented Lilly from obtaining patent protection over its insulin technology during the affected period. Faced with this severe version of compulsory licensing, the company was potentially discouraged from any innovation in insulin technology during the five-year period. Additionally, Lilly probably at least delayed patent applications until after the licensing period, relying instead on trade secret or other forms of protection. The one significant mitigating factor, however, was the license's provision that the licensee could be asked to contribute to the R&D expenses.[220]

Based on a few indicators, Lilly continued to aggressively pursue insulin R&D during the period covered by the license. For example, patenting behavior did not appear to be affected. The company filed for seven patents over the five-year licensing period, whereas fewer than seven patents were filed during the periods five years prior and subsequent to the licensing event combined.[221]

Several factors seemed to motivate Lilly's continued innovation during the licensing period. One is historical market leadership. The company's 1984 Annual Report states that "[w]ith our historical position in diabetes and the patients we serve, it is clear we have to aggressively go out and look at proinsulin. If it is potentially better, then we have an obli-

217. Because the license was made available to any domestic company with a bona fide intention to enter the insulin market, and the licensee did not require FTC approval, the FTC did not publicly track whether any licenses were implemented. The FTC would only have intervened had there been a complaint of non-compliance. Telephone Interview with Kenneth Davidson, Fed. Trade Comm'n Bureau of Competition (Apr. 26, 1995).

218. *See* ELI LILLY 1981 ANNUAL REPORT, *supra* note 149, at 5-6.

219. *See A Market Face-off for Two Insulin Pioneers*, *supra* note 150.

220. *See In re* Eli Lilly & Co., 95 F.T.C. 538, 1980 FTC LEXIS 85, *24 (1980).

221. Search using keyword "insulin."

gation to bring it forward. We owe this to society and humanity."[222] Another factor is that Lilly was an early leader in the research leading to the production of human insulin through recombinant DNA methods in 1978. Through subsequent testing and commercialization, the company was often first or second to introduce products of increasing purity to market.[223] Likewise, insulin was always one of Lilly's most important products. Shortly after the company took its first license in 1923, insulin accounted for half of all Lilly's profits, and in 1994, it was still the company's second largest revenue producer.[224]

Insulin continues to be a high revenue generator, despite being viewed as a commodity product due to significant barriers to entry such as the high cost of clinical trials for new biotechnology products and the cost of an efficient manufacturing facility.[225] Finally, Lilly continues to face continuous pressure from competitor Novo Nordisk; in 1980 the two companies together held nearly 80% of the insulin market (53% by Eli Lilly and 24% by Novo Nordisk), and by 1995, the two virtually split 91% of the market (Eli Lilly capturing 46% and Novo 45% of the market).[226] The pressures generated by market leadership, a desire for market dominance, and competition provided significant motivations for Lilly to continue to innovate, even during the compulsory licensing period.

D. Connaught/Rabies Vaccine

1. The Order

In 1992, citing concerns about increased domination of the U.S. rabies vaccine market, the FTC ordered Merieux to lease the rabies manufacturing business of the company it acquired, Connaught Bioscience.[227] Merieux was the sole supplier of rabies vaccine in the United States, and Connaught was one of two potential entrants into the market. Worried that Merieux's monopoly would remain unchallenged, the Commission called upon Merieux to lease Connaught's entire rabies vaccine manufacturing business, including both the production facility and technology, to an approved lessee for a minimum of twenty-five years.[228] In exchange, the or-

222. *See* ELI LILLY 1983 ANNUAL REPORT, *supra* note 152, at 17.
223. *See* CHRISTENSEN, *supra* note 151, at 1.
224. *See id.* at 1, 4.
225. *See id.* at 4.
226. *See id.* at 17, exh.9.
227. *In re* Institut Merieux S.A., 113 F.T.C. 742, 1990 FTC LEXIS 291,*8-9 (1990).
228. *Id.*

der provided for the lessee to give a lump sum payment, under customary and reasonable terms, to Merieux/Connaught.[229]

2. Subsequent Developments

Despite contacting twenty-eight prospective licensees over the next several years, including serious negotiations with a few parties, Merieux could not find a suitable buyer for Connaught's rabies manufacturing business.[230] The most serious offer, from North American Vaccine, Inc., was rejected because of a lack of relevant experience.[231] In April 1994, the FTC modified the original order and removed the leasing requirement, citing the entry of SmithKline Beecham into the market and Merieux's bona fide attempts to satisfy the consent decree.[232]

3. Impact on Innovation

During the period between the original and modified order, Merieux had little incentive to invest in Connaught's facilities, given that the order required it to lease the business away at uncertain prices. In fact, in the consent modifying order, Merieux suggested that "the continuing lease requirement may be harmful to competition . . . because it adversely affects Connaught's ability to respond to the increased demand for vaccine with capital investments to upgrade and expand the business's productive capacity."[233] Although evidence of this decline is not in the consent order, no patents were filed by the would-be leased Connaught for rabies vaccine inventions during the contested period, while five patent applications were filed by Connaught-Merieux, which ultimately became Aventis, in the subsequent years.[234]

Based on the evidence, it appears likely that Connaught's rabies vaccine practice suffered under this most extreme version of compulsory licensing. Given Connaught's position as a potential entrant in the U.S. market, the potential of enriching a competitor in the same market probably served as a major deterrent. Despite the continued interest of Merieux in the rabies business, little motivation may have existed for them to invest in Connaught. During the same interim period in which Connaught did not file for any patents, Merieux remained active in the rabies vaccine busi-

229. *Id.*

230. *In re* Institut Merieux S.A., 117 F.T.C. 473, 474-75 (1994) (modifying the 1990 order).

231. *Id.* at 476.

232. *Id.*

233. *Id.* at 477.

234. Search using keywords "rabies" and "vaccine" with incidental mentions screened out.

ness, launching a new product in 1992[235] and filing for a patent in late 1981. All of this is consistent with Merieux's statement to the Commission that the order adversely affected its incentives to maintain and improve the Connaught manufacturing capabilities.

E. Chiron/HSV-tk Related Therapeutics

1. The Order

In early 1997, the merger of Ciba Geigy, which owned the largest share of Chiron, and Sandoz concerned the FTC. Believing that the combination would create a "killer" patent portfolio[236] concerning the herpes simplex virus-thymidine kinase (HSV-tk) gene, the FTC ordered the companies to license their patent portfolios to an approved licensee.[237] The FTC was concerned that combining the patent portfolios would heighten already existing barriers to entry in the market for HSV-tk gene therapy, in which Chiron and Sandoz were leaders.[238] Anticipating that the combined portfolio would reduce the parties' incentives to license their patents, the order called for the licensing of other key gene therapy patents and divestitures in unrelated areas.[239] Unlike the other situations discussed here, this decision seemed to be openly motivated by protecting public health in addition to protecting competition. FTC Bureau of Competition Director William Baer even stated, "[t]his case is about saving lives. Today there are two firms racing to develop new gene therapies to combat deadly diseases. The deal threatened to eliminate that competition. Our order ensures that this sprint to the finish line will continue."[240]

The order required the merging parties to offer perpetual rights to their HSV-tk patent portfolios and provide related know-how to Rhone-Poulenc Rorer ("RPR") or another approved licensee. In order to ensure that a license would be issued, the FTC specified that compensation could be in the form of an equivalent cross-license or a royalty.[241] Within six months of the decree, the Commission approved the licensing of Chiron's

---

235. *See Merieux Doubles Profits, supra* note 160.

236. James B. Kobak Jr. & Richard P. McGuire, *FTC Looks at Merger's Antitrust Effects on R&D,* NAT'L L.J., Mar. 31, 1997, at C3.

237. *In re* Ciba-Geigy Ltd., 123 F.T.C. 842, 873-77 (1997).

238. *Id.* at 864-73, 877-86.

239. *Id.* at 846-47.

240. *See* Press Release, Fed. Trade Comm'n Office of Public Affairs, FTC Accord in Ciba Geigy/Sandoz Merger to Prevent Slowdown in Gene Therapy Development & Preserve Competition in Corn Herbicides, Flea-Control Markets (Dec. 17, 1996), *available at* http://www.ftc.gov/opa/1996/12/ciba.htm (last visited Aug. 27, 2003).

241. *In re* Ciba-Geigy Ltd., 123 F.T.C. at 873-77.

HSV-tk portfolio to multiple companies in fulfillment of the order.[242] In exchange, one licensee, Novartis, paid Chiron $60 million in addition to cross-licenses to some of its technologies.[243]

2. Impact on Innovation

Chiron's loss of exclusivity and "killer" patents over HSV-tk technologies potentially dampened its enthusiasm and willingness to invest in additional research. However, the opportunities presented by the cross-licenses given by Novartis, in addition to Chiron's market leadership position, probably mitigated any such effect. Chiron was likely not interested in scaling back research merely based on the speculative downstream impact of a licensee.

In the years following the order, Chiron continued to patent HSV-tk technologies at a rate comparable to its filings before the order.[244] Additionally, in 1998, the company reported that it had two products in development, one for graft-versus-host disease and another for hemophilia A.[245] Over the 2000 to 2002 period, Chiron and Novartis were involved in two of the fifteen trials reported in the Biospace CCIS database.[246] Meanwhile, licensee RPR, which became part of the larger pharmaceutical entity Aventis, appeared to make strides in the gene therapy market. The company launched RPR Gencell to develop gene therapies for cancer and other diseases in collaboration with other companies.[247] According to these measures, the license does not appear to have significantly harmed Chiron's innovation.

F. Roche/CD-4

1. The Order

In late 1990, the FTC ordered Roche, in connection with its acquisition of Genentech, to license its future rights to pending patents covering CD4-based technologies.[248] The order narrowly defined the relevant mar-

242. *See For Your Information*, Fed. Trade Comm'n Office of Public Affairs, Sept. 12, 1997, http://www.ftc.gov/opa/1997/09/petapp50.htm (last visited Aug. 11, 2003).

243. *See Chiron to License RPR for HSV-tk Gene and Cross-License Technologies with Ciba-Novartis*, BUS. WIRE, Dec. 17, 1996.

244. Search using keywords "gene therapy", "retroviral vector", and "HSV."

245. CHIRON CORP., 1998 ANNUAL REPORT 9 (1999).

246. Search using keyword "HSV."

247. Jim Papanikolaw, *Waiting for the Fruits of Gene Therapy*, CHEM. MKTG. REP., Mar. 20, 2000.

248. *In re* Roche Holding Ltd., 113 F.T.C. 1086, 1990 FTC LEXIS 543, *25 (1990).

ket as "CD-4 based therapeutics for the treatment of AIDS and HIV infection."[249] At the time, Genentech led the market with a product in clinical trials, with Roche following along with several patent applications. However, given the early stage of the technology, the merging parties were at most only potential competitors in the marketplace.[250]

The order provided perpetual access to Roche's patents in exchange for 1% of net sales for process patents and 3% of net sales for product patents. The license could be requested by any competitor or potential entrant over the ten years following the order, subject to its continuing commitment to CD4 research.[251]

2. Subsequent Developments

In the years following the order, Roche's patenting activity[252] far outperformed its pre-order levels. This is not surprising given that Roche only began to file for patents shortly before the order. In addition, the company remained committed to the investigation of CD4-based therapeutics in the treatment of AIDS. During the two-year period from 2000 to 2002, the company was a partner in four of the twelve clinical trials of drugs, three with Genentech and another with Baxter International.[253] Accordingly, the order did not significantly affect Roche's CD4 HIV research.

3. Impact on Innovation

To the extent that Roche relied on its patents to secure its competitive position in the CD4-based therapeutic market, the patent weakening license potentially discouraged Roche from investing as heavily as without the license. Even without the license, Roche presumably could have decided to abandon its own efforts relying instead on the innovation of leader Genentech. However, given the early stage of CD4 therapeutic development, Roche most likely decided that the compulsory license posed little threat in the ultimate therapeutic market.

---

249. *Id.* at *3.
250. *Id.* at *4.
251. *Id.* at *25-26.
252. Search using keywords "CD4" and "viral."
253. According to Biospace's CCIS database.

CYBERCRIMES & MISDEMEANORS: A REEVALUATION OF THE COMPUTER FRAUD AND ABUSE ACT

By Reid Skibell†

ABSTRACT

This Article contends that the Computer Fraud and Abuse Act is an overly punitive and largely ineffective approach to combating computer crime based on two fundamental critiques. The 1986 version of the CFAA contemplated a core distinction between harmless trespass and more substantial intrusions. Over time, this distinction has become obscured and is resulting in over-criminalization of offenders. Furthermore, the increased penalties for computer crime created by the USA PATRIOT Act, and the Cyber Security Enhancement Act, are unjust in application and ineffectual in deterring prospective computer criminals.

TABLE OF CONTENTS

---

† Reid Skibell is a J.D. Candidate at Columbia Law School, and has an M.Sc. in Information Systems from the London School of Economics. He has worked extensively in the technology industry, in both the United States and Europe. The author would like to specially thank Tugba Colpan and Andrea Skibell for their help in editing early drafts of the article, and John Dunagan for his assistance with technical computer security issues.

I. INTRODUCTION

When considering the nature and evolution of federal computer crime legislation, it is telling that the passage of the principal law for combating computer crime, the Computer Fraud and Abuse Act ("CFAA"),[1] was based in part on a fear derived from the movie WarGames,[2] which had been released the prior year.[3] That such a mundane movie could be the genesis of the U.S. computer crime laws is indicative of how, historically, there has been little connection between public policy and reality in this area of the law.[4] What makes this tendency so problematic is that policy-makers evince little concern for the practical effects that have resulted from strengthening the CFAA due to the high degree of consensus in the political community. The legislative history of the 1986 amendments to the CFAA, its first major reworking, contains detailed discussions on the proper limits to criminal liability and the appropriate role of government. The record reflects the careful planning, extensive debate, and compromises that went into crafting these revisions.[5] In this sense, the 1986 amendments are emblematic of a cautious approach to computer crime which seeks to flesh out the complexities of the issue. In contrast, the 2002 hearings on the Cyber Security Enhancement Act,[6] the most recent addition to the CFAA, read like an exercise in unanimity, demonstrating near universal agreement that computer crime is a significant and growing problem whose solution lies in aggressive criminal sanctions.[7] The degree

---

1. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2000).

2. WARGAMES (MGM/UA Studios 1983).

3. *See* Richard C. Hollinger & Lonn Lanza-Kaduce, *The Process of Criminalization: The Case of Computer Crime Laws*, 26 CRIMINOLOGY 101, 106-07 (1988) (explaining that surveys showed computer crime barely registered as a public concern prior to the movie but was found to be a serious one in its wake); Joseph M. Olivenbaum, *Rethinking Federal Computer Crime Legislation*, 27 SETON HALL L. REV. 574, 596 (1997) (noting the importance the movie played in the original debates on the CFAA).

4. For a full description of the progression of the social conception of the computer criminal, and how far removed it has become from what the available evidence suggests is the true nature of the computer criminal, see Reid Skibell, *The Myth of the Computer Hacker*, 5.3 INFO., COMM. & SOC'Y 336 (2002).

5. *See* S. REP. NO. 99-432, at 5-14 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482-92.

6. Homeland Security Act of 2002, H.R. 5710, 107th Cong. § 225 (2002) (Section 225 is known as the Cyber Security Enhancement Act of 2002).

7. *See Cyber-Security Enhancement Act of 2001: Hearing on H.R. 3482 Before the Subcomm. on Crime, House Comm. on the Judiciary*, 107th Cong. 17-19 (2002) [hereinafter *Hearing on H.R. 3482*] (statement of Alan Davidson, Staff Counsel, Ctr. for Democracy & Tech.), *available at* http://www.house.gov/judiciary/davidson021202.htm. The Center for Democracy and Technology ("CDT") was the lone opposition voice at the

of consensus was so pronounced that there was little, if any, debate on the proposed changes; and even traditional defenders of civil liberties like the Center for Democracy and Technology found few concerns over which to voice protest.[8] Congress has sought to strengthen the CFAA with every revision since 1986 by creating new crimes, lowering the required level of intent, and increasing the penalties. The consistency of this strengthening process prompted one court to conclucde that in interpreting the Act where there is ambiguity, Congress's intent should be presumed to enlarge the scope of the CFAA's reach.[9]

The CFAA is the cornerstone of the federal government's strategy for combating computer crime, and the punitive mindset upon which it is based is embedded within it and likely indicative of its future direction. The speed of technological change and the complexity of the new information economy demand a sophisticated treatment, but the appreciation of this complexity that was present in the 1986 amendments has been lost. This Article challenges this dominant computer crime paradigm, arguing that the current version of the CFAA is deeply flawed in how it categorizes and penalizes computer crime. Essentially, the original distinction between harmless computer trespass and felonious computer crime has been obscured, resulting in a misguided and ineffective computer crime policy. Part II traces the development of the CFAA, showing how the Act has evolved and explaining the rationale behind the many changes. Part III examines the world of the computer criminal, detailing the poor fit between the CFAA and the proper object of the legislation. Parts IV and V raise two primary objections to the Act's current structure and argue that this structure results in over-criminalization. Part VI analyzes the changes made to the penalty structure by the USA Patriot Act ("USAPA")[10] and the Cyber-Security Enhancement Act and argues that the proper ends of the criminal justice system are not furthered by excessively harsh sanctions for computer crime. Finally, Part VII concludes that a return to a more balanced approach, as embodied by the 1986 version of the CFAA, is necessary to create a more just and effective national computer crime policy.

---

hearing and their only criticism had to do with the Internet Service Provider provisions of the law, not ones concerning cybercrime.

8. *Id.*

9. *See* United States v. Middleton, 231 F.3d 1207, 1212 (9th Cir. 2002) ("Congress has consciously broadened the statute consistently since its original enactment.").

10. United and Strengthening America by Providing Appropriate Tools by Providing Appropriate Tools Required to intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 [hereinafter USAPA], *available at* http://www.eff.org/Privacy/Surveillance/Terrorism_militias/hr3162.pdf.

II. THE EVOLUTION OF THE COMPUTER FRAUD AND ABUSE ACT

In 1984, Congress hastily drafted and passed the CFAA. At the time, the Act was widely criticized as being overly vague and too narrow in scope.[11] In light of these deficiencies, Congress undertook a more careful study of computer crime and completely revised the Act in 1986.[12] Since then, the CFAA has been amended eight more times during its relatively short lifespan. An appreciation of the Act's history is necessary to understand the problems with the current version. Rather than attempt to detail the extensive number of small changes that have been made, this Article focuses on those that have proven most important in practice.

In devising the structure of the 1986 Act, a key Congressional concern was differentiating between computer trespass and more damaging types of computer crime.[13] Part of the rationale for this distinction was a belief that the law's focus should be on combating computer abuses that would either result in significant economic harm or threaten the integrity of sensitive data. There was also a generalized concern about over-prosecution and Congress felt that the division between computer trespass and felonious computer crime would be an effective means to curb excessive use of the Act.[14] One example of how Congress attempted to build this understanding into the CFAA is the addition of the trespass provision found in subsection (a)(3). By creating subsection (a)(3), Congress criminalized all unauthorized access to federal computers but decided it would be improper to classify such access as more than a misdemeanor.[15] It also limited the definition of trespass to attacks by outsiders, even though such a

---

11. *See* Dodd S. Griffith, Note, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 466-67 (1990) (noting the widespread dissatisfaction with the original 1984 Act).

12. *Id.* at 474-82.

13. S. REP. NO. 99-432, at 9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2487.

14. This distinction is emphasized in a number of places within the legislative history. For example, in discussing the intent requirement of subsection (a)(4) it was noted that, "The Committee remains convinced that there must be a clear distinction between computer theft, punishable as a felony, and computer trespass, punishable in the first instance as a misdemeanor." *Id.* at 10, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2488. It also makes the distinction when explaining that consuming time on a system does not qualify as having defrauded the system's owner of anything: "[I]t is important to distinguish clearly between acts of fraud under (a)(4), punishable as felonies, and acts of simple trespass, punishable in the first instance as misdemeanors." *Id*. Similar wording is also used to describe why merely obtaining knowledge of how to break into a system is also not a fraud. *Id.*

15. *Id*. at 10-11, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2488.

limitation would create a gap in the reach of the Act.[16] Congress viewed the creation of the trespass offense as a compromise that provided "the best means of balancing the legitimate need to protect the Government's computers against the need to prevent unwarranted prosecutions of Federal employees and others authorized to use Federal computers."[17] In this manner, Congress sought to send the message that illegally accessing a federal computer is a crime, but limited the penalty to a level that properly reflected the insubstantial nature of the offense.

The 1986 amendments also enlarged the scope of the CFAA by creating three new felony offenses: computer fraud, trafficking in network passwords, and hacking.[18] Subsection (a)(4) created a federal computer fraud offense, but Congress distinguished computer fraud from mail and wire fraud by mandating that using a computer was a requirement for criminal liability.[19] The fraud subsection also contained a computer use exemption, which stipulated that the value of computer time used by the hacker while inside the foreign system was not to be treated as a fraud. Congress was concerned that a simple trespass might be turned into felony fraud based on the economic value of the computer time.[20] Congress also created a second new offense, subsection (a)(6),[21] making it a crime to traffic in network passwords.[22] The most important addition was the creation of a hacking offense, subsection (a)(5), intended to penalize those who damaged or altered the data of another. All three of the new offenses required damages exceeding $1,000 to become a felony, unless a violation of subsection (a)(5) involved the alteration of medical records.[23] These three new offenses included a mens rea of "intentionally," a higher re-

16. An outsider is anyone who intrudes on a computer from outside the organization, as opposed to an insider who exceeds their authorized access by viewing sensitive data or entering into a restricted computer. The CFAA in 1986 only covered "federal interest computers," and the insider-outsider distinction was based on whether or not the attacker worked for the government. Consequently, the Act would not apply in the rare case of an intradepartmental trespass. *See id.* at 8, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2486.

17. *Id.*

18. *Id.* at 9, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2487.

19. *See id.* ("The Committee does not believe that a scheme or artifice to defraud should fall under the ambit of subsection (a)(4) merely because the offender signed onto a computer at some point near to the commission or execution of the fraud.").

20. *See id.* at 10, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2487 ("[The trespass/felony distinction] would be wiped out were the Committee to treat every trespass as an attempt to defraud a service provider of computer time.").

21. 18 U.S.C. § 1030(a)(6).

22. S. REP. NO. 99-432, at 13, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2490-91.

23. *Id.* at 12, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2490.

quirement than the level of "knowingly" which was used throughout the 1984 version of the CFAA.[24] The intent threshold was also raised in other parts of the Act; the rationale was that those who might mistakenly access a protected computer or stumble upon another's data protection should be exempted from liability.[25]

The Act was modified in minor ways in 1988, 1989, and 1990 to clarify certain terms. The next significant change came in 1994. Subsection (a)(5) was rewritten to create two new offenses. The first offense covered intentional acts, which remained a felony, and the second created a misdemeanor crime for merely reckless acts. This misdemeanor crime was a departure from the 1986 Act, which did not criminalize unintentional damage caused while accessing a system.

There were some practical problems prosecuting cases under the CFAA during the first ten years of the Act's existence. During this time, a generalized concern about the growing seriousness of computer crime was also forming.[26] Consequently, the CFAA was fully revised in 1996, establishing the law's current structure. The compromises that had been written into earlier versions of the CFAA were largely abandoned in favor of a broad expansion of the Act. For example, the subsection (a)(3) federal computer trespass provision was expanded to apply to government insiders as well as outsiders and the computer use exception was deleted from the (a)(4) fraud subsection.[27] These earlier compromises had not proven to be a significant handicap to prosecutors,[28] thus the compromises' elimina-

---

24. *See id.* at 10, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2488.

25. *See id.* at 5-6, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2483-84

26. *See* Haeji Hong, Note, *Hacking Through the Computer Fraud and Abuse Act*, 31 U.C. DAVIS L. REV. 283, 290 (1997) (explaining that expanding the scope of the Act was the major impetus for the manifold changes made).

27. Computer Crime & Intell. Prop. Section, U.S. Dep't Justice, *Legislative Analysis of the 1996 National Information Infrastructure Protection Act*, *at* http://www.usdoj.gov/criminal/cybercrime/1030_anal.html (last modified June 10, 1998) [hereinafter CCIPS, *Legislative Analysis*].

28. Evidence for this comes from the fact that none of the cases listed as being pursued by the DOJ include "computer use" as the basis for the crime. *See* Computer Crime & Intell. Prop. Section, *Computer Intrusion Cases*, *at* http://www.cybercrime.gov/cccases.html (last modified July 8, 2003) [hereinafter CCIPS, *Computer Intrusion Cases*]. Also, the DOJ admits that the change to section (a)(3) was not really necessary. *See* CCIPS, *Legislative Analysis*, *supra* note 27 ("While this defense would almost have negated the law and thus defied a common-sense interpretation of the former law, Congress added the word 'non-public' to make it perfectly clear that a person who has no authority to access any non-public computer of a department or agency may be convicted under (a)(3) even though permitted to access publicly available computers.").

tion without a specified need is illustrative of just how thoroughly the Act was altered in 1996.

Another type of change involved "loopholes" that prosecutors had identified as potentially problematic.[29] Congress's approach to fixing these possible holes marked a sharp departure from its handling of the 1986 amendments. Instead of balancing the state's interest against the threat of over-criminalization as was done in 1986, Congress used wording that expanded the scope of the Act as far as possible. For example, Congress found that a definition of "damage" was necessary because the 1994 amendments were written to require both "damage" and "loss," and there was a concern that in some cases there might be evidence of financial losses but not sufficient permanent damages to fall under the Act.[30] Congress defined "damage" in two ways. First, damage included any impairment to a system. Second, damage could be any harm which the Act prohibited.[31] Congress intentionally refrained from making a list of prohibited actions to avoid being under-inclusive.[32] Congress intended any ambiguities in drafting to be interpreted in favor of prosecutors.

The 1996 amendments also completely restructured subsection (a)(5), creating three offenses: two felonies and one misdemeanor. Congress changed the Act to cover a wide range of crimes and thus applied a different mens rea to each offense.[33] The first felony, codified in subsection (a)(5)(A), covered anyone who intentionally damages a computer by knowingly transmitting a harmful program. This subsection contained the highest mens rea of the three newly created offenses and is the only one that applies equally to insiders or outsiders.[34] The second felony subsection applies to those who intentionally access a computer without authori-

---

29. *See* CCIPS, *Legislative Analysis*, *supra* note 27 (arguing for the need to amend the CFAA).

30. *See id*.

31. *Id.* ("In addition, Congress has listed two new threshold harms in its definition of 'damage': causing physical injury to any person [18 U.S.C. § 1030(e)(8)(c)] and threatening the public health or safety [18 U.S.C. § 1030(e)(8)(c)]."). It should be noted that the definition of "damage" as "threatening the public health or safety" was codified at 18 U.S.C. § 1030(e)(8)(d).

32. *See id*. ("The statutory language avoids listing specific acts that can cause such impairment to insure that its coverage is suitably broad.").

33. *See* ORRIN HATCH, THE NATIONAL INFORMATION INFRASTRUCTURE PROTECTION ACT OF 1995, S. REP. NO. 104-357, at 11 (1996) (outlining the restructuring of § 1030(a)(5)), *available at* ftp://ftp.loc.gov/pub/thomas/cp104/sr357.txt.

34. *See id.* at 2; *see also id.* at 11 (explaining that § 1030(a)(5)(A) applies to insiders and outsiders).

zation and recklessly cause damage.[35] Determining that the culpability of criminal trespass was sufficient to make reckless damage a felony, Congress purposely lowered the mens rea for external attacks.[36] Finally, the third subsection imposes a misdemeanor penalty on intentionally accessing a computer without authorization and negligently causing damage.[37]

The only limitation provided to counterbalance the expansion of the Act was raising the jurisdictional damage level from $1,000 to $5,000.[38] This monetary threshold is the only difference between a felony offense and a misdemeanor for an external attacker who recklessly or intentionally causes damage. The $5,000 floor can also be waived upon proof of physical injury to any person or if public safety is threatened.[39] This change has not proven to be significant to prosecutions under the CFAA.[40]

In the wake of the 9/11 tragedy, Congress passed the USAPA[41] which contains provisions directed at combating the threat of cyberterrorism. These provisions changed the CFAA by making it easier to charge computer criminals with a felony. First, Congress mandated that $5,000 in damage did not have to be shown if the computers attacked were used for national security or criminal justice.[42] Congress also changed two sections to make it easier to reach the felony monetary threshold. As the only criminal court to define "loss" under the CFAA, the Ninth Circuit in *United States v. Middleton*[43] adopted a definition that arguably went be-

35. *See id.* at 10 ("Subsection 1030(a)(5)(B) would penalize, with a fine and up to 5 years' [sic] imprisonment, anyone who intentionally accesses a protected computer without authorization and, as a result of that trespass, recklessly causes damage.").

36. *See id.* at 11 ("[I]t is equally clear that anyone who knowingly invades a system without authority and causes significant loss to the victim should be punished as well, even when the damage caused is not intentional.").

37. *See id.* at 11-12 ("Finally, subsection 1030(a)(5)(C) would impose a misdemeanor penalty, of a fine and up to 1 year imprisonment, for intentionally accessing a protected computer without authorization and, as a result of that trespass, causing damage. This would cover outside hackers into a computer who negligently or accidentally cause damage.").

38. *See* CCIPS, *Legislative Analysis*, *supra* note 27 (arguing that the increased importance of computers in the economy meant that it was proper to raise the threshold of what constituted significant financial losses).

39. *See* HATCH, *supra* note 33, at 13-19.

40. This is clear from the DOJ's list of cases prosecuted under the CFAA. *See* CCIPS, *Computer Intrusion Cases*, *supra* note 28.

41. USAPA, *supra* note 10.

42. *See* Computer Crime & Intell. Prop. Section, *Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001*, *at* http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm (last updated Nov. 5, 2001) [hereinafter CCIPS, *Field Guidance*].

43. 231 F.3d 1207 (9th Cir. 2000).

yond the 1996 amendments by including the cost of damage assessments and any lost revenue or costs associated with an interruption in service.[44] Congress subsequently endorsed this interpretation of "loss" by codifying it into the new law.[45] The second change involved allowing the damage from a single attack to be aggregated across many computers.[46] Thus, a virus causing only minimal damage to any given infected computer but contaminating a large number of computers could reach the felony monetary threshold.[47]

The USAPA also raised the penalties for violating the CFAA's felony provisions. The maximum punishment for first-time offenders was raised from five to ten years. In the case of repeat offenders, the maximum punishment was raised from ten to twenty years, and a new provision was inserted that allowed related state convictions to be counted as prior offenses.[48] The newly passed Cyber Security Enhancement Act complements the USAPA in directing the Sentencing Commission to upgrade the seriousness of penalties assessed under the CFAA.[49] The Commission responded to this directive by changing the guidelines in April 2003, guaranteeing that those convicted of computer crimes would face substantially increased penalties.[50]

III. WHAT EXACTLY IS A "HACKER"?

Part of Congress's rationale in taking a more punitive approach to cybercrime has been that the quality of the threat has changed and the penalties should rise accordingly to meet this new danger. Representative Lamar Smith, Chairman of the House Subcommittee on Crime, effectively conveys this perspective:

> America must protect our national security, critical infrastructure, and economy from cyber attacks. Penalties and law en-

---

44. *Id.* at 1210-11.

45. *See* CCIPS, *Field Guidance*, *supra* note 42 (arguing that the changes "codify the appropriately broad definition of loss adopted in [*Middleton*]").

46. *Id.*

47. *Id.*

48. *Id.*

49. *See* Computer Crime & Intell. Prop. Section, *Amendments & Redline Showing Changes Resulting from Sections 225 and 896 of the 2002 Homeland Security Act*, *at* http://www.usdoj.gov/criminal/cybercrime/homeland_225.htm (last updated May 19, 2003).

50. *See* Patricia Manson, *Panel OKs Tougher Federal Sentencing Rules*, CHI. DAILY L. BULL., Apr. 21, 2003, at 1 (giving some examples where the penalties would double under the new guidelines).

> forcement capabilities must be enhanced to prevent and deter such criminal behavior. Until we secure our cyber infrastructure, a few keystrokes and an Internet connection is all one needs to disable the economy or endanger lives. A mouse can be just as dangerous as a bullet or a bomb.[51]

Smith's comments are representative of the change in focus of computer crime laws, particularly after 9/11. Essentially, the CFAA has become narrowly focused on combating a certain type of computer criminal. However, the individuals that fall under the current scope of the CFAA are not limited to malevolent intruders and cyberterrorists. This profound over-simplification of the cybercriminal archetype goes to the heart of this Article's critique.

The computer underground lexicon generally divides computer criminals into three separate types: script-kiddies, hackers, and crackers.[52] The first group carries out the majority of computer intrusions. Script-kiddies employ tools downloaded from the Internet to exploit common security weaknesses. They have limited programming knowledge and commit very basic errors, like trying to execute UNIX commands on machines not running UNIX-compatible operating systems. Consequently, a significant portion of the damage that they cause is unintentional as script-kiddies are prone to making mistakes especially when starting out.[53] Because the programs they use are generally geared toward nuisance crimes like defacing a website rather than to more serious crimes like stealing sensitive data, the amount of damage this first group can do is usually limited. Furthermore, Martin Caminada, whose study of security incidents within Dutch

---

51. *Hearing on H.R. 3482*, *supra* note 7, at 2 (statement of Rep. Lamar Smith, Chairman, Subcomm. on Crime of the House Comm. on the Judiciary).

52. To this third group can be added cyberterrorists who have traditionally not been included in discussions of the computer underground. Crackers and cyberterrorists are similar in that that they are both motivated by something more than the thrill of breaking into foreign systems. The reason that cyberterrorists are not a part of the traditional lexicon is that their very existence is doubtful. *See infra* note 62 and accompanying text.

The other category of person prosecuted under the computer crime laws are corporate insiders, but their motivations and method of attack make them distinct from the computer criminals analyzed in this paper. A computer may be the means for the commission of their crime, but they should not be understood as computer criminals. *See* Skibell, *supra* note 4, at 353.

53. *See* Richard Barber, *Hackers Profiled—Who Are They and What Are Their Motivations?*, COMPUTER FRAUD & SEC., Feb. 2001, at 14; Editorial, *Hackers, Crackers and Phreakers Oh My!*, COMPUTER FRAUD & SEC., Apr. 1999, at 18 (script-kiddies make very common programming mistakes with regularity); Duncan Graham-Rowe, *Access Granted*, NEW SCIENTIST, Aug. 12, 2000, at 42 ("[Script-kiddies have] no idea what they're doing. They download programs or scripts and hack by pointing and clicking.").

corporations, is noteworthy for the depth of information they were able to solicit from attacked companies, found that properly deployed firewalls helped minimize the damage that these types of attackers could do.[54] However, some of the tools script-kiddies utilize are quite powerful, and it would be a mistake to assume they are only capable of minor vandalism. This group is also important because hackers and crackers usually begin as script-kiddies before advancing to the other groups.[55]

The second type of computer intruder is the hacker, distinguished as being more experienced and possessing more programming skills than a script-kiddie. Hackers are able to use the standard tools with a much higher degree of sophistication and some are adept enough to design intrusion programs.[56] The cracker shares the hacker's sophistication, but the difference lies in motivation. For hackers, the desired reward is the hack itself because of the rush involved in breaking into what was thought to be a secure system.[57] There is also a voyeuristic component, as hackers often describe themselves as being drawn to the power of being able to see what is hidden from the general populace.[58] While this motivational distinction between hackers and crackers may appear subtle, it is crucial to understanding that hackers pose a relatively insubstantial criminal threat to companies and institutions.

Though hackers may be skilled, available evidence suggests that they pose a rather limited criminal threat. Paul Taylor's research on the computer underground community found that hackers have little interest in pursuing financial or ideological goals. What motivates them to attack a given target is the opportunity to boast that they have conquered it.[59]

---

54. Martin Caminada et al., *Internet Security Incidents: A Survey Within Dutch Organizations*, 17 COMPUTERS & SEC. 417, 425-26 (1998); Telephone Interview with Dr. John Dunagan, Microsoft Researcher, Microsoft Corp. (Dec. 28, 2002) (explaining that technology is making it increasingly difficult to illegally access sensitive data); *see also* Wade Roush, *Hackers: Taking a Byte Out of Computer Crime*, TECH. REV., Apr. 1995, at 32 (firewalls and related technology protects sensitive data from external attacks).

55. *See* Barber, *supra* note 53, at 15.

56. DOUGLAS THOMAS, HACKER CULTURE 43-44 (2002); Barbara, *supra* note 53, at 15.

57. PAUL A. TAYLOR, HACKERS: CRIME IN THE DIGITAL SUBLIME 56-58 (1999). Taylor's research is noteworthy for its extensive interviews with computer intruders and the insider perspective he was able to uncover.

58. *Id.*

59. *Id.* at 59-61; *see also* Tom Mulhall, *Where Have All the Hackers Gone? Part 3—Motivation and Deterrence*, 16 COMPUTERS & SEC. 291, 293-97 (1997); Emmanuel Goldstein, *Q&A with Emmanuel Goldstein of 2600: The Hacker's Quarterly*, CNN INTERACTIVE, Mar. 22, 2002, *available at* http://www.cnn.com/TECH/specials/hackers/qandas/goldstein.html (defining hacking as an "inquisitive" activity); Mark Ward, *Sabo-*

Douglas Thomas makes an even stronger argument. He found that the talented hackers who could pose the greatest threat are the ones who also tend to be the most concerned with ethical issues. Thomas argues that, "[skilled hackers] tend instead to be the most strongly motivated by an ethic which values security, which values information, and which puts innovation and learning at the top of their list of priorities."[60] Taylor and Thomas have performed the most extensive academic work to date on the computer underground, thus their assessment of the criminal potential of hackers should be given substantial weight. Furthermore, Caminada's empirical research lends support to this view of hackers as benign. They conclude that the majority of computer intruders have no interest in damaging the systems they penetrate. Specifically, they found that, "[n]ot a single responding organization mentions incidents in which the perpetrator has read or modified any truly sensitive data, such as customer files or financial data."[61]

The real danger from computer crime comes from the third category of intruders that includes crackers and cyberterrorists. Crackers include those who attack computer systems for personal profit, such as people carrying out economic espionage, or for malicious purposes, like virus writers. Cyberterrorists are grouped with crackers because they share similarly malevolent purposes, but they still remain a theoretical threat. To date, there is no evidence of any cyberterrorists currently operating. Although much has been written about the threat from this third group, there are good reasons to believe that the threat is overstated, particularly the specter of cyberterrorism.[62] While a full examination of the subject is beyond the scope

---

tage in Cyberspace, NEW SCIENTIST, Sept. 14, 1996, at 12 (describing hackers as motivated primarily by curiosity).

60. *Cyber Terrorism and Critical Infrastructure Protection: Hearing Before the Subcom. on Gov't Efficiency, Fin'l Mgmt. and Intergovernmental Relations of the Comm. on Gov't Reform*, 107th Cong. (2002) [hereinafter *Critical Infrastructure Protection Hearing*] (statement of Douglas Thomas), *available at* http://www-rcf.usc.edu/~douglast/testimony.pdf.

61. Caminada, *supra* note 54, at 423; *see also* TAYLOR, *supra* note 57, at 21-22 (arguing that crackers are a very tiny group existing only on the fringes of the digital underground).

62. I have dealt with this subject at length, arguing that the societal vision of the dangerous computer intruder is not borne out by reality. While the statistics on the surface show an economic threat from crackers, a careful analysis shows the danger is substantively inflated. *See* Skibell, *supra* note 4, at 347-53. Joshua Green effectively makes a similar case against cyberterrorism. Green concludes that:

> There is no such thing as cyberterrorism—no instance of anyone ever having been killed by a terrorist (or anyone else) using a computer. Nor is there compelling evidence that al Qaeda or any other terrorist organi-

of this Article, an observation made by the respected political scientist Murray Edelman is enlightening. Edelman noted that the public image of small outsider groups is particularly vulnerable to being exploited politically because these groups have no political constituency and the public has little contact with them.[63] The characteristics of the digital criminal community closely correspond to Edelman's criteria. The media portrayal and societal image of the computer criminal have also shifted markedly over the last twenty years.[64] In a short period of time, the public's perception of the computer criminal has gone from harmless, socially awkward nerd to dangerous cyberterrorist, leaving the question as to how much, if any, of this change reflects reality, and how much is a creation of symbolic politics.

The combination of the composition of the computer underground and the Edelman hypothesis suggests that there is a severe mismatch between the mythical computer criminal targeted by the increasingly-strict CFAA changes and actual perpetrators who are at risk of prosecution under the Act. This disparity between the imagined and the real criminal threat has substantial consequences in light of the broad reach of the law's felony provisions. This Article now turns to explaining how the legal distinction between benign trespass and harmful cracking has been virtually written out of the Act, thereby allowing all categories of computer criminals to fall under the harsh penalties of the CFAA.

> zation has resorted to computers for any sort of serious destructive activity. What's more, outside of a Tom Clancy novel, computer security specialists believe it is virtually impossible to use the Internet to inflict death on a large scale, and many scoff at the notion that terrorists would bother trying.

Joshua Green, *The Myth of Cyberterrorism*, WASH. MONTHLY, Nov. 2002, at 8, *available at* http://www.washingtonmonthly.com/features/2001/0211.green.html; *see also Critical Infrastructure Protection Hearing* (statement of Douglas Thomas), *supra* note 60, at 5 ("The reality is that there is very little that a well-funded terrorist group could do that a 16-year-old hacker couldn't. And neither of them threatens us in a way that can rightly be called 'terrorism.'"); Scott Berinator, *The Truth About Cyberterrorism*, CIO MAG., Mar. 15, 2002, *available at* http://www.cio.com/archive/031502/truth.html (stating that data might be threatened but infrastructure attacks are too difficult); Ward, *supra* note 59 at 12.

63. MURRAY EDELMAN, THE SYMBOLIC USES OF POLITICS 1-13 (1964).

64. Skibell, *supra* note 4, at 343-347; *see also* TAYLOR, *supra* note 57, at 7-11; THOMAS, *supra* note 56, at 219; Amanda Chandler, *The Changing Definition and Image of Hackers in Popular Discourse*, 24 INT'L J. SOC. OF LAW 229, 249-50 (1996) (concluding that hacking, which used to attract "sneaky admiration" is now viewed as treacherous).

IV. COPYING OF FILES AND THE TROPHY PROBLEM

The first major problem with the CFAA concerns the copying of files by computer hackers. As previously explained, the locus of hacker activity is the thrill of breaking a system's security. This experience regularly includes copying files as a token or trophy of the conquest. Often, there will be no intent on the part of the intruder to sell or otherwise benefit from the copied material and the intrusion will cause no actual damage to the system. This behavior can be analogized to someone breaking into the Louvre and making a perfect digital copy of the Mona Lisa to hang in her bedroom, leaving the physical picture unblemished. Certainly, there is a difference between how society would want to treat such a criminal and how it treats someone that steals the Mona Lisa itself. In terms of utility, stealing the painting deprives another party of valuable property and inflicts a corresponding injury on the community by decreasing the overall incentive to produce works of art. This behavior should be prohibited not only for reasons of individual fairness, but because societal utility is threatened. In contrast, copying the Mona Lisa represents an infringement upon an individual's right to exclude, but the harm to society is far less clear. The harm from copying is of a significantly lesser degree. Copying a painting is closer to the crime of trespass then it is to the crime of fraud or theft. Both types of behavior are worthy of punishment, but it is a mistake to treat them identically.

The trophy issue has proven to be problematic in computer crime prosecutions because the government has had mixed success proving that the victim has been deprived of something valuable. In an early 1990 computer crime prosecution, Craig Neirdorf was accused of causing $80,000 worth of harm to AT&T by posting an illegally obtained sensitive internal document on his electronic bulletin board. During the trial it was revealed that the same information was publicly available for a mere $13 to anyone who wrote to AT&T.[65] Neirdorf was acquitted of all charges but, in a more recent case, "notorious" computer hacker Kevin Mitnick was not as fortunate. Mitnick broke into the computers of Sun Microsystems and downloaded the Solaris operating system source code for which Sun ("Sun") had paid $80 million. He plead guilty so the CFAA's reach was not directly implicated, but he received a harsh punishment under the sentencing guidelines because he was charged with causing damage equal to the value of the software. Mitnick had no intention of altering or selling the code. Indeed, there was no genuine damage done to Sun besides public

65. BRUCE STERLING, THE HACKER CRACKDOWN: LAW AND DISORDER ON THE ELECTRONIC FRONTIER 276-77 (1993).

embarrassment.[66] In fact, Sun never reported any loss to its insurance company, the IRS, or its shareholders, casting further doubt on the validity of the damages figure used to calculate Mitnick's penalty.[67] In an interesting parallel to the Neirdorf case, Sun made the code publicly available for a mere $100 soon after the break-in.[68] The only place that the $80 million damages figure ever existed was in the trial record, yet that was sufficient to have severe consequences for Mitnick.

The copying of proprietary data is covered by 18 U.S.C. § 1030(a)(4), the computer fraud provision. This subsection criminalizes accessing a computer without authorization and with the intent to defraud, obtain, or attempt to obtain, anything worth more than $5,000.[69] This provision was designed to "penalize thefts of property via computer that occur as part of a scheme to defraud."[70] An example of the type of crime the drafters had in mind is setting up a webpage that mirrors a large e-commerce site for the purpose of acquiring credit card numbers. Fraud is a zero-sum game, with gains to one party coming at the expense of another. Mitnick's crime does not fit comfortably into this conventional conception of fraud, since he obtained something of substantial value but has not deprived his victim of anything. Consequently, he arguably does not possess the requisite mens rea, or criminal purpose, for the crime of fraud. However, the Supreme Court in *Carpenter v. United States*[71] determined that a fraud can be perpetrated without any monetary damage. The Court ruled that a newspaper, *The Wall Street Journal*, had the exclusive right to determine how its confidential information is disseminated, thus a scheme that would infringe on that property right can be classified as fraud.[72] To the extent that a computer intrusion invariably involves a violation of the victim's

66. David Banisair, *Computer Hacker's Sentence Spotlights High-Tech Crime Prosecutions*, CRIM. JUST. WKLY., Aug. 3, 1999, *available at* http://packetstorm.icx.fr/mag/hwahaxornews/HWA-hn31.txt (last visited Aug. 24, 2003).

67. Douglas Thomas, *How Much Damage Did Mitnick Do?*, WIRED, May 5, 1999, http://www.wired.com/news/politics/0,1283,19488,00.html.

68. *See* Lindsey Arent, *Did Sun Inflate Mitnick Damages?*, WIRED, May 22, 1999, http://www.wired.com/news/politics/0,1283,19820,00.html.

69. 18 U.S.C. § 1030 (a)(4) (2000).

70. S. REP. NO. 99-432, at 9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2486-87.

71. 484 U.S. 19 (1987).

72. *Id.* The principal defendant, Foster Winans, an employee of *The Wall Street Journal*, was the author of a widely read column that tended to increase the stock price of companies which he highlighted as good buys. The scheme involved his releasing the names of companies in the column early to stockbrokers who would buy the stocks ahead of the market. They would then sell the stocks and Winans would realize a portion of the profits. *Id.*

right to exclude, *Carpenter* most likely means that any copying of a trophy will be regarded as fraud.

The originator of the scheme in *Carpenter*, Foster Winans, intended to profit from his employer's property, even though it was not his purpose to directly harm the newspaper.[73] Winans was able to do this because the information had a value outside of the context of the newspaper; it allowed someone to trade in front of information that would most likely drive up the price of a stock. This reveals a crucial difference between *Carpenter* and the Mitnick case: Mitnick had no intent to personally profit and, indeed, it would have been extremely difficult to realize a gain even if he had tried. The data that Mitnick stole had no value outside of the context of Sun. This is true of most, but not all, types of information that hackers might copy. There is also a distinction with regard to the victims' relationship to the information. In *Carpenter*, the value of *The Wall Street Journal*'s property interest was directly related to its exclusivity.[74] If the knowledge contained in the column were widely distributed, then investors who might have otherwise purchased the paper would have no interest in reading about these "hidden gems." In contrast, the fact that Sun started giving away the code for a negligible amount to developers and educational institutions demonstrates that exclusivity did not have the same primary relationship to the information's value.

Some support for these differences comes from the First Circuit's decision in *United States v. Czubinski*,[75] which distinguished *Carpenter* in important ways. The defendant, Richard Czubinski, used his job at the IRS to view confidential taxpayer data, though he never disclosed the data to third parties or made practical use of it.[76] Dismissing the wire fraud and computer fraud violations against Czubinski, the court classified his behavior as "idle curiosity" that broke departmental rules but did not rise to the level of fraud.[77] The court held that fraud requires that "either some articulable harm must befall the holder of the information as a result of the defendant's activities, or some gainful use must be intended by the person accessing the information, whether or not this use is profitable in the eco-

73. *Id.* at 23 (noting that the net profits of the scheme amounted to over $690,000).

74. *Id.* at 28.

75. 106 F.3d 1069 (1st Cir. 1997).

76. *Id.* at 1072. Czubinski was a member of a white supremacist organization and the government was probably expecting to locate evidence that he used his access to the IRS data to further that cause. *Id.* However, it turned out that Czubinski only abused his position to do things like run credit checks on his girlfriend. *Id.*

77. *Id.* at 1078.

nomic sense."[78] The logic of the court's reasoning fits the circumstances of the trophy problem, where there is no intention to make use of the copied data. Admittedly, in assessing the computer crime charge, the court attached some weight to the fact that Czubinski never downloaded or printed out any of the data he viewed, but the court made its observation in the context of establishing that Czubinski's purpose was benign. Similar to Czubinski, hackers like Mitnick are primarily guilty of curiosity which, even if it should be punishable, does not deserve to be classified as felonious criminal fraud.

One reason that *Czubinski* has not been helpful to cybercriminals is that the First Circuit's focus on intent has been largely disregarded, as demonstrated in *United States v. Ivanov*.[79] The court stated that the crucial difference with *Czubinski* was that the defendant, Aleksey Ivanov, was not merely viewing the data but had control over it because he had obtained root access to the system.[80] Root access is a descriptive term meaning that the user is recognized as a system administrator and consequently obtains the authority to change passwords or destroy data–authority that normal users do not have. Root access is used to commit computer crime in many instances, but prior to *Ivanov* it was not regarded as sufficient evidence to ensure a fraud conviction under the CFAA.[81] The defendant in *Czubinski* had similar authorization to copy or destroy the IRS data, thus the court's decision in *Ivanov* clearly increases the relevance of the intruder's level of access. However, the case has not been criticized and it is a telling example of how courts are reading *Czubinski* as narrowly predicated on the defendant's physical relationship to the data.

---

78. *Id*. at 1074.

79. 175 F. Supp. 2d 367 (D. Conn. 2001).

80. *Id.* at 371-72. Ivanov was a Russian national, and the case was litigated before the CFAA was explicitly expanded extra-territorially. The "under control" theory used by the court is largely for the purposes of getting around this jurisdictional problem, but its interpretation of *Czubinski* is still problematic.

81. Congress seemingly addressed the issue of root access in the 1986 amendments, and the relevant sections of the CFAA have not been changed. The legislative history explains that simply accessing a system is not sufficient to qualify as having "obtained" anything:

> In intentionally trespassing into someone else's computer files, the offender obtains at the very least information as to how to break into that computer system. If that is all he obtains, the offense should properly be treated as a simple trespass. But because the offender has obtained the small bit of information needed to get into the computer system, the danger exists that his and every other computer trespass could be treated as a theft, punishable as a felony under this subsection.

S. REP. NO. 99-432, at 9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2486-87.

Another reason that *Czubinski* will not be followed comes from a 1996 change that allows a different part of the CFAA to reach the copying of data. Based on the Tenth Circuit decision in *United States v. Brown*[82] that the interstate theft provision in § 2314 does not include intangible information,[83] Congress expanded § 1030(a)(2) by making it a felony to obtain information involved in interstate communication worth more than $5,000 or to use such information for financial gain.[84] It is particularly noteworthy that Congress chose § 1030(a)(2) as the means to deal with this hole in the law because when this subsection was created in 1986 it was intended only to cover the extraordinary situation where the illegally obtained information was either financial records or confidential government documents.[85] Because of the sensitive nature of financial and governmental information, merely viewing the documents is sufficient to damage the party that owns the data. Consequently, Congress made clear that asportation, or removing the data from its original location, was not required for a conviction.[86] Furthermore, the information that subsection (a)(2) originally covered was of such a private nature that there was no reason to add a monetary threshold to that subdivision, whereas subsection (a)(4) already had one. By expanding (a)(2) instead of changing (a)(4), Congress equated obtaining data with viewing it in many contexts where it made little sense to classify the underlying behavior as a crime of conversion.

V. MENS REA AND THE $5,000 THRESHOLD

One of the key changes in the 1996 reformation of the CFAA was the division of the subsection (a)(5) anti-hacking provision into three separate offenses based on intent.[87] This portion of the Act is the one most widely used in criminal prosecutions, but neither Congress nor the courts have grappled with the important question of what distinguishes computer hacking that is merely negligent from that which is reckless. The crime of hacking, which by its very nature involves intentionally breaking security

82. 925 F.2d 1301 (10th Cir. 1991).

83. *See* CCIPS, *Legislative Analysis*, *supra* note 27 (the change was based upon the *Brown* decision).

84. *See id*. ("Moreover, consistent with Congress's prior construction of § 1030(a)(2), 'obtaining information' includes merely reading it; i.e., there is no requirement that the information be copied or transported. This is critically important because, in an electronic environment, information can be 'stolen' without asportation, and the original usually remains intact.").

85. S. REP. NO. 99-432, at 6, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2489.

86. *Id.*

87. *See* HATCH, *supra* note 33, at 11.

to traipse around a foreign system, would seem to involve an inherent and foreseeable risk of causing accidental damage. The logical distinction between the two may be difficult to establish in practice and the mens rea requirement might not provide sufficient protection against over-criminalization. Some commentators also argue that judges commonly lack detailed technical knowledge and consequently have a tendency to overestimate the abilities of computer hackers.[88] While this finding is far from conclusive and it is unclear how such misconceptions would affect the conduct of a trial or the creation of jury instructions, judges may view even unsophisticated script-kiddies under a stringent "reasonable person" standard thus making recklessness far easier to prove. If the negligence/recklessness distinction does not prevent relatively harmless computer intrusions from becoming felonies then the only safeguard against broad application of the two (a)(5) felony provisions is the monetary requirement. Consequently, proper calculation of damages accrued in the course of a computer intrusion is of central importance in ensuring appropriate punishment under the CFAA.

Since the 2001 USAPA changes, calculation of damages under the Act has been based on the reasoning in *Middleton*, which held that loss under the statute includes anything that was the natural and foreseeable result of the intrusion, as well as the costs to repair and "resecure" the system against future intrusions.[89] This figure includes lost profits. Courts have determined lost profits to include damages for loss of goodwill and reputation.[90] Losses can also be aggregated, meaning that instances of minimal damage to multiple computers can be added together to surpass $5,000.[91] This expansive definition of damage essentially makes the $5,000 threshold meaningless. The result is that computer hackers are at the mercy of prosecutors because almost any computer intrusion can be charged as a felony under the CFAA's anti-hacking provisions.

---

88. *See* TAYLOR, supra note 57, at 2-5 (on the example of Kevin Poulsen and Chris Lamprecht's skills being overestimated); R.U. Sirius, *Superhacker Kevin Mitnick: Menace to Fear or Rogue to Love?*, VILLAGE VOICE, Feb. 22, 1999, *available at* http://www.villagevoice.com/issues/0007/sirius.php (on the example of Kevin Mitnick's skills being overestimated).

89. United States v. Middleton, 231 F.3d 1207, 1213 (9th Cir. 2000).

90. *See, e.g.*, Ingenix, Inc. v. LaGalante, 2002 U.S. Dist LEXIS 5795, at *26, *29 (E.D. La. Mar. 28, 2002); *In re* America Online, Inc., 168 F. Supp. 2d 1359, 1380 (S.D. Fla. 2001); Compuserve Inc. v. Cyber Promotions, 962 F. Supp. 1015, 1023 (S.D. Ohio 1997). *But cf.* United States v. Pierre-Louis, 2002 WL 1268396, at *2 (S.D. Fla. Mar. 22, 2002) (admitting the 2001 Patriot Act changes the law on this point). The *Ingenix* opinion was removed from the Lexis Service at the request of the court on August 25, 2003.

91. 18 U.S.C. § 1030(a)(5)(B)(i).

A. The Problem of "Resecuring" Costs

In cases involving destruction of property, cost of repair is a common way for courts to determine whether a jurisdictional threshold has been exceeded. As an example, take *Nichols v. United States*,[92] which involved a common liquor store robbery. In *Nichols* the magnitude of the loss was determined by calculating the cost of fixing the roof and interior door that were physically damaged in the course of entering the establishment.[93] It is fair to assign the blame for this damage to the perpetrators of the crime, since their direct actions caused the damage to the store.

The 1986 amendments used a conception of loss similar to *Nichols*. Loss was based on the costs of actual repairs and on the costs incurred during reprogramming or restoring data to its original condition.[94] Costs of repairing the security hole that the attacker used to penetrate the system would not be covered but expenses related to returning the company to its position prior to the incident would be.[95] The 1986 version of the Act also included reliance damages, such as those incurred by an investor who mistakenly invests in a stock based on information contained in an altered database, in the damage calculation.[96] Since the loss is easy to demonstrate and the harm results directly from the actions of the intruder, this inclusion is not a significant departure from the formula used in the destruction of property example. On the other hand, damages for reputational and customer goodwill losses, recovery for which was added in 1996, are particu-

---

92. 343 A.2d 336 (D.C. App. 1975).

93. *Id.* at 341-42. *Nichols* was chosen as a representative destruction of property case because of its clear and reasoned approach to how to perform a damage calculation. It has also been somewhat influential, having been cited in other jurisdictions, including Alabama, Idaho, Illinois, and Maryland. *See* Cartee v. State, 390 So. 2d 1121, 1124 (Ala. Crim. App. 1980); State v. Hughes, 946 P.2d 1338, 1343 (Idaho Ct. App. 1997); People v. Carraro, 394 N.E.2d 1194, 1196 (Ill. 1979); Robinson v. State, 468 A.2d 328, 323 (Md. 1983).

94. *See* S. REP. NO. 99-432, at 11 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2488-89.

95. This is based on my reading of the 1986 legislative history. No court has made a determination about whether the 1986 version of the CFAA covers the costs of "resecuring," namely those involved in fixing the security weakness used by the attacker. The closest a court came to a ruling on this issue was in *United States v. Sablan*, where restitution only included costs strictly related to repairing the damaged files. United States v. Sablan, 92 F.3d 865, 870 (9th Cir. 1996) ("The consequential expenses incurred due to the meetings with the FBI, the staff meeting, and the handling of the crank calls were not expenses necessary to repair the files damaged by Sablan's criminal conduct. These expenses were thus not properly included in the restitution order.").

96. S. REP. NO. 99-432, at 11, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2489.

.

larly difficult to quantify and partial responsibility may lie with the victim company.[97] However, certain types of computer crime, like website defacement, target a company's reputation. Computers are of central importance to businesses and reputation is an important and fragile asset. Thus, inclusion of these costs might thus be justified as an attempt to specifically deter a particularly damaging and malicious type of computer crime.

What is far more difficult to defend is the inclusion of "resecuring" costs, which are the expenses derived from fixing the security hole that the hacker used to access the system. While Congress has never addressed the rationale behind making the intruder liable for these expenses, the *Middleton* court did. The court reasoned that patching the hole is necessary to make the hacked corporation whole, much like fixing the door and roof for the liquor store owner. This figure should not include improvements to the system, but should only make the system as secure as it was before the attack.[98] The problem with this line of reasoning is that it assumes that a computer intruder does damage when they break into a system when, in reality, all they are doing is exploiting a pre-existing weakness or hole in the security of the system. The company was not more secure before the attack—just because no one had chosen to enter did not mean that the door was not wide open. Consequently, "resecuring" by definition includes an improvement to the system, fixing a weakness that was there long before the intruder exploited it.

The court in *Middleton* also pointed out that the eminent foreseeability of resecuring made it fair to include resecuring costs in the damage assessment.[99] However, it is also predictable that the owner of the liquor store in the *Nichols* case would respond to the physical break-in by reinforcing the interior door, improving the locks, and adding a security system; yet none of this is attributed to the thief. Because the choice of the proper level of security lies with the owner of the store, society does not see fit to blame the thief for these costs. The owner of a store is certainly aware of the possibility of a robbery and his decision on the appropriate

---

97. This will be explained in greater detail in Part VI.C, but the victim company may have consciously elected to not address known weaknesses and thus might not be justified in claiming that the computer criminal tarnished their reputation for taking security seriously.

98. United States v. Middleton, 231 F.3d 1207, 1213 (9th Cir. 2000); *see also In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 521 (S.D.N.Y. 2001) ("S. Rep. No. 104-357 seems to make clear that Congress intended the term 'loss' to target remedial expenses borne by victims that could not properly be considered direct damage caused by a computer hacker."); Shurgard Storage Ctr. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Wash. 2000) (justifying the inclusion of investigation costs).

99. 231 F.3d at 1213.

level of security is independent of the thief's actions. Yet in the context of computer crime, the CFAA makes the intruder liable for the corporation's negligence in haphazardly guarding their own data. Surveys indicate that the majority of companies are aware of the weakness in their own security but choose to ignore the danger.[100] Companies often under-invest in security for financial reasons but there is also widespread carelessness such as when people fail to update software or ignore internal security guidelines.[101] Perhaps there is an argument to be made that the sophisticated hacker should be held liable for resecuring a system, as they may have used their skills to penetrate a system that was reasonably secure. However, the unfairness of the CFAA is evident in the case of script-kiddies, whose sole ability to break into a system is predicated on using a standardized program to exploit a commonly known security weakness. The CFAA would make them guilty of a felony, or enhance their punishment under the sentencing guidelines, simply because a corporation failed to address serious holes in its own security.

Another reason that resecuring should not be included in damage assessments from hackings is the disjuncture between the locus of the underlying crime and the origin of the costs of resecuring. When network security is found to be compromised, a system administrator will generally respond by trying to trace back how the intruder was able to gain access.[102] When the security weakness is found and neutralized, the administrator's job is not yet complete. A good administrator must check the security of all devices or parts of the network that had a relationship with the part compromised to ensure that those related devices do not possess a similar vulnerability. The theory is that all possible sources of entry must be examined before the system can again be declared secure.[103] Companies are also increasingly collecting evidence to use against the intruder as part of their overall response to an attack.[104] The formation of companies special-

100. *See, e.g.*, Stephen Hinde, *Security Surveys Spring Crop*, 21 COMPUTERS & SEC. 310, 314 (2002); Richard Power, *2002 CSI/FBI Computer Crime and Security Survey*, 8 COMPUTER SEC. ISSUES & TRENDS, Spring 2002, at 1.

101. Hinde, *supra* note 100, at 314.

102. *See* Dunagan, *supra* note 54; Jim Yuill et al., *Intrusion-Detection for Incident-Response: Using a Military Battlefield-Intelligence Process*, 34 COMPUTER NETWORKS 671, 671-672 (2000) (explaining the standard response to an intrusion).

103. *See* Dunagan, *supra* note 54 (stressing that the system must be pronounced free of newly introduced holes, known as "Trojans," before a security incident can be classified as concluded).

104. In *Sablan*, the court specifically rejected inclusion of investigation expenses. United States v. Sablan, 92 F.3d 865, 870 (9th Cir. 1996); *see supra* note 95 and accompanying text. However, that was under the 1986 version of the Act. In the recent *LaGal-*

izing in computer forensics has accelerated this trend. Such information-gathering activities are not even tangentially related to the attacker's culpability, however these companies contend that the gathering of evidence to be used against the attacker is part of containing the damage of a computer intrusion. Computer hackers are thus being criminally charged based on the cost of their victim's investigations.

What makes blaming hackers for these types of costs so problematic is how expensive they are relative to the felony monetary threshold. Jennifer Granick, a former computer crime defense attorney, contends that a large proportion of the costs calculated under the CFAA are due to work that bears little or no relationship to the actual attack.[105] Though it is a civil case, *EF Cultural Travel v. Explorica, Inc.*[106] is indicative of the type of abuse to which she is referring.[107] No actual harm was done to Explorica but the court still found a violation of the CFAA because of the high cost of diagnostic testing. Specifically, Explorica spent $20,944.92 to determine if there was any damage and over $40,000 to resecure their website and network.[108]

---

ante case, a former employee who was accused of stealing sensitive data was assigned the cost of hiring a computer forensic specialist who helped collect the evidence used against that former employee. Ingenix, Inc. v. LaGalante, 2002 U.S. Dist LEXIS 5795, at *26-27 (E.D. La. Mar. 28, 2002). This trend is likely to continue as investigations for the purpose of repairing the system, and for the purpose of collecting evidence against the attacker, are merging together in the IS community. This is particularly true in the case of outside specialists, who argue that properly containing the internal damage and public relations dangers from an intrusion involves gathering evidence. The already tenuous distinction between repairing and improving a system is further called into question by this development. *See, e.g.*, Berni Dwan, *Nowhere to Hide*, COMPUTER FRAUD & SEC., Dec. 2002, at 13; Michael Goldberg, *Watching the Detectives: Computer Forensics can Help Companies Uncover the Digital Truth*, CIO MAG., June 1, 2002, *available at* http://www.cio.com/archive/060102/et_note.html; Cliff May, *Computer Forensics–the Morse or Clouseau Approach?*, COMPUTER FRAUD & SEC., Nov. 2002, at 14; Deniz Sinangin, *Computer Forensic Investigations in a Corporate Environment*, COMPUTER FRAUD & SEC., June 2002, at 11.

105. Telephone Interview with Jennifer Granick, Director, Stanford Law School Center for Internet and Society (Nov. 4, 2002). Because so few criminal computer crime cases ever make it to trial, Granick was invaluable in providing practical information on how these prosecutions are handled.

106. 274 F.3d 577 (1st Cir. 2001).

107. Given the relative paucity of criminal decisions under the CFAA, civil cases provide important evidence of how courts are interpreting its provisions.

108. *Explorica*, 274 F.3d at 584.

B. The Problem of Calculating Intangible Harms

A separate problem involves the reliance on loss estimations from companies that have been hacked. While certain aspects of a company's response to an intrusion are standard, the reality is that the amount of time spent responding can vary widely depending on the capabilities of the IT staff, whether the company utilizes specialized assistance, and the company's general level of experience with security incidents.[109] According to Granick, a company responding to a website defacement might assess anywhere between one to forty hours of repair time.[110] Given this lack of uniformity, it is very difficult for a defendant to contest this portion of a company's estimate. More intangible aspects of the cost calculation, such as damage to reputation and lost productivity due to network downtime, are even harder for a defendant to dispute given their speculative nature. The 2002 CSI/FBI Computer Crime Survey reported that 80% of respondents had experienced financial losses emanating from computer attacks, but only 44% could quantify their losses.[111] This is a significant gap and coming from an anonymous survey it demonstrates how hard it is to compute intangible losses accurately. Even when companies list these types of losses, accuracy remains questionable. Thomas Varney, a former Secret Service agent specializing in computer crime provides an instructive example: "A company calls up and says, 'We've just been hacked. We've lost $1 million.' They pull a number out of the air . . . I ask how they got that number, and it turns out they're just guessing."[112] Conceivably, the difficulty of calculating intangible harm could benefit computer crime defendants because they would be able to cast doubt on any figure that a company might produce. In practice, however, this has not been the case. Courts have interpreted the CFAA to include these types of costs, despite their inexact nature. Courts have also been reluctant to let doubtful cost estimates benefit defendants and have shown deference to the calculations of victim corporations.[113]

---

109. Companies, particularly those that are smaller or have never previously experienced an attack, generally respond in an ad hoc and disorganized manner. Simone Kaplan, *It's Not Easy Being Breached*, CSO MAG., Dec. 2002, http://www.csoonline.com/read/120902/cost.html; May, *supra* note 104, at 14; Sinangin, *supra* note 104, at 12.

110. Granick, *supra* note 105.

111. Power, *supra* note 100, at 11. Forty-four percent was the highest percentage of respondents who could quantify their losses in the survey's seven years.

112. Kaplan, *supra* note 109.

113. Granick, *supra* note 105 (explaining that corporations have been expected to provide little, if any, documentation of their costs).

Allowing companies to define the damage they have suffered is dangerous because they have an incentive to choose a figure in excess of $5,000. A large proportion of computer crimes are perpetrated by disgruntled or former employees who use their knowledge to bypass the company's security measures.[114] In such a situation, executives may construe the intrusion as personal and thus may be encouraged to inflate the damage assessment in a vindictive attempt to get back at the employee. For example, in *Ingenix, Inc. v. LaGalante*, the defendant refused to return a laptop to his former employer and proceeded to download sensitive data that he intended to use to ingratiate himself to a competitor.[115] Though it was prosecuted as a civil case, Ingenix estimated the cost of examining the laptop at $7,000 and was given wide flexibility to determine their business losses from the copied data.[116] In a criminal trial, the $7,000 would have been sufficient to ensure that LaGalante faced a serious felony conviction. LaGalante's former employer could easily have retaliated against him by being extra diligent in examining the laptop and thereby inflating their costs to surpass $5,000.

There is also reason to believe the FBI is encouraging companies to inflate their damage assessments. Jennifer Granick reports that the FBI regularly informs companies that there must be over $5,000 in damages in order to warrant prosecution. She believes that this prompting is responsible for many of the high estimates of damage from computer intrusions.[117] While Granick can only speak to her own experience, there is circumstantial evidence that this practice is widespread. *2600: The Hacker Quarterly*, a journal devoted to computer hacking, has letters on its website purported to be communications between the FBI and executives of companies that have been hacked.[118] These letters demonstrate that the monetary figure chosen for the actual harm from incidents was always computed after consultation with law enforcement, rather than being a figure that was determined prior to companies' awareness of the legal importance of their calculations.

---

114. Eric Shaw et al., Dep't of Def. Sec. Inst., *The Insider Threat to Information Systems: The Psychology of the Dangerous Insider*, SECURITY AWARENESS BULL., Sept. 1998, at 1, 7.

115. 2002 U.S. Dist LEXIS 5795 (E.D. La. Mar. 28, 2002).

116. *Id.* at *26-27.

117. Granick, *supra* note 105.

118. *New Mitnick Evidence Reveals Corporate Fraud,* 2600: THE HACKER Q., Apr. 22, 1999, *at* http://www.2600.com/news/display/display.shtml?id=357. *2600: The Hacker Quarterly* is the main periodical devoted to computer hacking and has a good reputation for the general quality of its information.

VI. THE USAPA AND THE PUNITIVE APPROACH TO CYBERCRIME

In addition to strengthening the internal provisions of the CFAA, Congress has increased the penalties for cybercriminals who run afoul of the Act's provisions. The USAPA makes these penalties particularly severe with up to ten years for a first violation and twenty years for a repeat offender.[119] The Act was intended to counter the threat from malevolent foreign crackers and cyberterrorists, whose very existence is not even established. Despite these goals, the real world impact of these new penalties will be on far less exotic computer criminals. These penalties are substantial. They are a product of a mindset that morally and instrumentally justifies strong criminal sanctions in the fight against computer crime. This Article next looks into the question of whether the twin goals of deterrence and retribution are furthered by the criminal sanctions that are now attached to the CFAA.

A. Deterrence and the Utilitarian Justification for High Penalties

It is highly doubtful that the USAPA will be successful in deterring the criminals who motivated its drafting. The nature of terrorism is such that it attracts passionate adherents, so the threat of criminal sanctions is not likely to dissuade such actors from their causes. Not all terrorists are willing to be suicide bombers, but their commitment is usually sufficiently strong to be uninfluenced by the computer crime laws of the United States. While the USAPA does add extraterritorial jurisdiction to the CFAA and there have even been a few successful prosecutions of foreign nationals, the level of international coordination and resources necessary to track down foreign computer criminals makes it doubtful that this type of prosecution will be commonplace.[120] The likelihood of being prosecuted under the CFAA is so remote that higher penalties will not sufficiently impact the decision calculus of foreign crackers. Thus, the two groups most feared by those advocating stiffer penalties are the ones least likely to be influenced by the USAPA changes.

Higher penalties might still be justified if they successfully cut down on more commonplace types of computer crime, but such a reduction in crime seems doubtful. The Antiterrorism and Effective Death Penalty Act of 1996 directed the Sentencing Commission to examine the deterrent ef-

---

119. USAPA, *supra* note 10, § 814(c)(3) (codified at 18 U.S.C. § 1030(c)(4)(A), (C) (2000)).

120. *See* Bill Boni, *Crossing the Line or Making the Case?*, COMPUTER FRAUD & SEC., Dec. 2002, at 18, 19 (relating the numerous obstacles to effectively pursuing foreign computer criminals).

fect of the CFAA. After a review of the then-available data and the general scholarship on deterrence, the Commission concluded that there was insufficient data to reach a conclusion on the deterrent effect of criminal sanctions.[121] The report stressed that the effectiveness of deterrence is contextual and that speculation about deterrence is difficult because of the inherent dissimilarities between the various individuals grouped under the rubric of computer crime.[122] In all likelihood, there is not enough information available on the psychology of computer criminals and other variables to make a declarative statement about deterrence. However, there is some evidence available that suggests that deterrence is not very effective in the context of computer crime.

Deterrence theory needs to account for the empirical evidence that nineteen years under the CFAA has done little to slow the growth of computer crime.[123] A common response is that the Act has always been plagued by poor draftsmanship and insufficient criminal penalties, which have rendered it ineffective. Despite these problems, the community of computer criminals is small and the message that computer crime is a serious offense should have been sufficiently communicated to this group by now. Between 1992 and 1998, 196 people were convicted of computer crimes, with 84 receiving prison sentences.[124] This is not an insignificant number. Based on these figures it should be obvious to all interested parties that the legal system regards computer crime as a serious offense, worthy of incarceration. Additionally, a number of these prosecutions, such as those of Kevin Mitnick and Kevin Poulsen, were high profile and received widespread media attention.[125] It seems reasonable that the shift

---

121. *See* U.S. SENTENCING COMM., REPORT TO CONGRESS: ADEQUACY OF FEDERAL SENTENCING GUIDELINE PENALTIES FOR COMPUTER FRAUD AND VANDALISM OFFENSES 9 (June 1996), *available at* http://www.ussc.gov/r_congress/COMPFRD.PDF ("The limited empirical data available to the Commission and other factors preclude a definitive assessment of the deterrent effect of existing guidelines for computer fraud and computer vandalism.").

122. *See id.* ("[R]esearchers who have studied general deterrence have found that it is very difficult to say with certainty the extent to which a given criminal sanction discourages criminal conduct."); *see also* Sanford Sherizen, *Can Computer Crime Be Deterred?*, 6 SEC. J. 177, 180 (1995) ("As difficult as deterrence is to apply, computer crime makes an even more difficult target.").

123. *See* Power, *supra* note 100, at 11 (survey results indicate that the amount of damage grew in comparison to past years).

124. *See* Banisair, *supra* note 66 (based on the statistics released under the Freedom of Information Act).

125. Wade Roush makes the interesting point that the criminal seriousness of computer hacking was apparent even before the Mitnick and Poulsen cases. *See* Roush, *supra* note 54, at 32. He finds that the 1989-1990 FBI crackdown on computer crime, Operation

in penalties from parole to jail time in most computer crime cases is a more powerful signal to would-be computer criminals than the change from five to ten years of jail time. Despite these signals, the anticipated decrease in computer crime has not come, a trend that has not been confined to the U.S. experience. Britain, Malaysia, and Singapore all have strong computer crime legislation, but the computer crime rates of all three countries continue to climb.[126]

One explanation for the unabated increase in computer crime is that not enough time has passed to see the effects of deterrence on computer criminals. Essentially, it is unfair to assess the success or failure of substantial penalties until a generation has matured under them. This point may have the most relevance with regard to script-kiddies, the group most likely to internalize a prohibition against hacking. They are casual participants in computer crime and their lower level of connection to the activity means that it may eventually be possible to inculcate a different set of values. However, their youth and general lack of sophistication also make them unlikely to consider the consequences of their actions, even the potential for significant jail time. While high penalties might eventually influence script-kiddies, any visible effect would likely take a long time to manifest.

Given the psychology of hackers and crackers, there is reason to believe that these categories of more dedicated computer interlopers will not be deterred by significant criminal penalties. Indira Carr and Katherine Williams contend that hackers are drawn to the mental challenge of bypassing security and as such do not utilize the cost-benefit analysis that underlies deterrence theory. Essentially, the only way these individuals feel they can prove their intellectual prowess is through hacking, so they will continue to do so regardless of the potential consequences.[127] One source of support for this argument comes from Paul Taylor's study of the hacking community. Taylor found that hackers have diverse motivations, but did not find any hackers who were motivated by the practical gains

---

Sundevil, sufficiently conveyed the message to the cybercrime community that hacking cases would be prosecuted and would likely result in incarceration. *Id.*

126. Indira Carr & Katherine S. Williams, *Securing the E-Commerce Environment: Enforcement Measures and Penalty Levels in the Computer Misuse Legislation of Britain, Malaysia and Singapore*, 16 COMPUTER LAW & SEC. REP. 295, 304 (2000).

127. Indira Carr & Katherine S. Williams, *A Step Too Far in Controlling Computers?: The Singapore Computer Misuse (Amendment) Act 1998*, 8 INT'L J.L. & INFO. TECH. 48, 56 (2000) (through their analysis is of the Singapore Act, they make this point generally); *see also* Raju Chebium, *Experts Say More Laws Won't Stop Computer Hackers*, CNN INTERACTIVE, May 8, 2000, *at* http://www.cnn.com/2000/LAW/05/05/love.bug/.

derived from breaking into computers. Instead, the hackers were driven by more benign motivations such as curiosity, feelings of power, and the camaraderie of belonging to a community.[128] In contrast, crackers hope to profit from their computer crimes, although this does not mean that personal enrichment is their sole motivation. They are often just as enamored with the mental challenges involved in breaking into secure systems as hackers, and financial gains are generally a secondary concern.[129] Furthermore, many hackers and crackers describe the mental rush of the activity as being so powerful that it is beyond their control. They are addicted to hacking.[130] It is probably premature to categorize hacking as a physical addiction, however, there is sufficient support for this proposition for Paul Bedworth to successfully raise addiction as a defense in the first trial under the UK's Computer Misuse Act.[131] Bedworth was so pathologically beholden to hacking that he would lock himself in his room and stay fixated on his computer for days until he dropped from exhaustion.[132] Not every computer criminal will demonstrate this degree of attachment, but the Bedworth example does suggest that the cost-benefit foundation of deterrence theory may be ill-suited to the context of computer crime.

B. The Negative Side Effects of High Penalties

Another problem with deterrence is that it ignores the makeup the hacker community. The main reason that hackers do not intentionally damage networks or commit fraud is a type of communal boundary formation.[133] Hackers do not see themselves as criminals and enforce a code of conduct that functions as a form of self-regulation. By not distinguishing between types of computer intruders and their crimes, the recent changes to the law will likely alienate hackers. Should hackers perceive that they are victimized by an unfeeling legal system where the punishment is not commensurate with the crime, this boundary formation may slip away. Such a process may have already started, as the hacker community was incensed by the legal system's treatment of Kevin Mitnick and responded

---

128. TAYLOR, *supra* note 57, at 46.

129. *Id.* at 19-22.

130. *Id.* at 46-50; *see also* Tom Mulhall, *Where Have All the Hackers Gone? Part 5—Conclusions*, 16 COMPUTERS & SEC. 304, 305 (1997) (Mulhall believes that legislation does have a deterrent effect, but finds it is undercut to a large degree by addiction).

131. *Id.*

132. Gillian Harris, *Daring Data Raider Dependent on Hacking Fix*, THE SCOTSMAN, Mar. 18, 1993.

133. TAYLOR, *supra* note 57, at 25-26; *see also* THOMAS, *supra* note 56, at 110 (arguing that the hacker ethic not only exists but is strengthening as the community has become more political).

in an uncharacteristically organized and political fashion.[134] This anger need not necessarily take a political form. Taylor found that hackers are under increasing pressure from third parties to use their skills for more traditionally criminal ends.[135] The potential now exists for an alienated hacker community to turn to more destructive crimes in response to the new penalty levels.

There are other indications that high penalty levels may actually exacerbate the problem of computer crime. It is generally accepted that the threat of being hacked has led to a revolution in computer security, forcing software companies to pay attention to the problem of how to effectively safeguard data.[136] Computer hackers play an under-appreciated role in raising awareness of security issues. The threat they pose has been instrumental to the development of new technologies such as encryption and biometrics.[137] On the surface, this situation appears analogous to other criminal endeavors—certainly the threat of bank robbery has lead to the creation of better safes. The crucial difference is that there is not a benign form of bank robbery. Software producers do not want to be embarrassed by having hackers effortlessly break the security they have designed. As a result, the threat of benign hacks has probably been responsible for advances in software design and testing that are working to counter much more dangerous computer intrusions. Thus, software producers' reaction to the threat of hackers, i.e., working to counter more dangerous computer intrusions, differs with other types of crime which only spur countermeasures designed to protect against the original crime.

Hackers have also been successful in pointing out security problems and suggesting improvements. On this point, Douglas Thomas notes, "hacks are often discovered, reported, and patched by hackers themselves without ever using them to compromise someone else's computer or security."[138] Hackers frequently help to close the very holes that crackers and

---

134. THOMAS, *supra* note 56, at 232.

135. TAYLOR, supra note 57, at 19-22 (arguing that criminal groups are starting to draw upon the skills of hackers).

136. *See* JOHN VIEGA & GARY MCGRAW, BUILDING SECURE SOFTWARE: HOW TO AVOID SECURITY PROBLEMS THE RIGHT WAY 15-16 (2002) ("[Software vendors] start to worry about security only after their product has been publicly (and often spectacularly) broken by someone.").

137. *See* Liz Duff & Simon L. Gardiner, *Computer Crime in the Global Village: Strategies for Control and Regulation—in Defence of the Hacker*, 24 INT'L J. SOC. L. 211, 220 (1996).

138. THOMAS, s*upra* note 56, at 43.

cyberterrorists could exploit in pursuit of their criminal objectives.[139] Because hackers are attracted by the mental challenge of testing supposedly-secure systems or widely disseminated products such as Microsoft products, their contribution to system patches and product improvements is significant. Consequently, increasing the punishments for benign intrusions might actually be detrimental to the overall goal of reducing the damage from computer crime.

A final argument against increased sentences for computer crime comes from an interesting parallel with the war on drugs. An examination of the cases currently being pursued by the Department of Justice reveals that the majority of people who are indicted for computer crimes are either company insiders or unsophisticated computer users.[140] The preponderance of these types of cases may be due to the targeting of low-level offenders. This problem frequently occurs in the drug context. High mandatory minimum sentences for distribution of drugs encourage prosecutors to go after mules rather than the drug kingpins because mules are easier to catch yet still receive a serious sentence.[141] This does not impute cynicism or maliciousness to criminal justice professionals, but prosecutors are judged by their conviction rate and the distinction between morally guilty and provably guilty is often blurred.

---

139. This role is particularly important given the significant number of security holes in most software products. *See, e.g.*, Abner Germanow et al., *The Injustice of Insecure Software*, @Stake Research Report (@stake, New York, NY), Feb. 2002, *available at* http://www.atstake.com/research/reports/acrobat/atstake_injustice.pdf (explaining that most applications are full of security holes); Rebecca T. Mercuri, *Security Watch: Computer Security Quality Rather than Quantity*, 45 COMM. OF THE ACM 11, 12 (October 2002); Bruce Schneier, *Foreword* to JOHN VIEGA & GARY MCGRAW, BUILDING SECURE SOFTWARE: HOW TO AVOID SECURITY PROBLEMS THE RIGHT WAY, at xix (2002) ("[T]he average large software application ships with hundreds, if not thousands, of security related vulnerabilities.").

140. The last statistics released on computer crime prosecutions under the CFAA are from 1998, so these releases represent the best available evidence of what types of offenders are being targeted. *See* CCIPS, *Legislative Analysis*, supra note 27. While the alleged amount of damage caused by the computer criminals seems to be extensive, the estimates are questionable as a number of them parallel the trophy problem demonstrated in the Mitnick and Neirdorf cases. Granick concurs with this assessment, as she believes that in these releases the DOJ is substantially inflating the harm caused. *See* Granick, *supra* note 105.

141. For a detailed analysis of how higher penalties that were supposed to be reserved for high-level offenders actually lead to greater targeting of low-level offenders in the drug context see U.S. SENTENCING COMMISSION, REPORT TO CONGRESS: COCAINE AND FEDERAL SENTENCING POLICY (May 2002), *at* http://www.ussc.gov/r_congress/02crack/2002crackrpt.pdf.

Prosecutors are often under pressure to take only cases that will result in conviction and incarceration. Susan Kelley Koeppen, a former federal prosecutor, makes the point that the decision whether to investigate and prosecute a given cybercriminal is often based on the perceived possibility of a stiff sentence:

> I speak from my own experience in saying that cyber criminals often don't get punished, because the applicable sentencing guidelines focus primarily on economic harm which is often difficult to calculate and may not reflect the true harm caused. Because these crimes do not merit stiff sentences, they may, in turn, not be investigated or prosecuted.[142]

Koeppen believes the solution is to make it easier to get harsh sentences by adjusting the sentencing guidelines, but perhaps it would be wiser to maintain the high threshold of culpability for severe penalties. The Department of Justice admits that it faces numerous obstacles to catching sophisticated cybercriminals, raising the possibility that resources could be shifted towards pursuing script-kiddies, who are now eligible for sufficiently long sentences.[143] Prosecution of script-kiddies represents a temptation, law enforcement's path of least resistance, but hardly a solution to the problem of computer crime.

There are also organizational tendencies that increase the potential for a focus on prosecuting low-level offenders. Because they are immersed in a world of crime, criminal justice professionals tend to employ cognitive maps which are rigidly bifurcated between good and bad. David Wall provides an example: "[F]or the police, objectives and places having routine uses are conceived of in terms of favorite misuses. Garbage cans are places in which dead babies are thrown, schoolyards are places where mobsters hang out, stores are places where shop lifters go, etc."[144] Apply-

142. *Hearing on H.R. 3482*, *supra* note 7, at 8 (statement of Susan Kelley Koeppen).

143. *Internet Denial of Service Attacks and the Federal Response: Hearing Before the Subcomm. on Crime, House Comm. on the Judiciary and the Subcomm. on Criminal Oversight of the Senate Comm. on the Judiciary*, 106th Cong. (2000) (statement of Eric Holder, Deputy Attorney General), *available at* http://www.usdoj.gov/criminal/cybercrime/dag0229.htm (explaining the technical and resource hurdles to catching sophisticated computer criminals); *see also* Marc D. Goodman, *Why the Police Don't Care about Cybercrime*, 10 HARV. J.L. & TECH. 465, 483-488 (1997); David S. Wall, *Catching Cybercriminals: Policing the Internet*, 12 INT'L REV. L., COMPUTERS & TECH. 201, 211 (1998).

144. Wall, *supra* note 143, at 212 (quoting Howard Sacks, *Notes on Police Assessment of Moral Character*, *in* STUDIES IN SOCIAL INTERACTION 292 (D. Sudnow ed., 1972)).

ing these studies to cybercrime, Wall concludes that criminal justice professionals mentally group hackers together; the negative characteristics that they possess as a class are attached to all individuals categorized as belonging to that class irrespective of experience, potential for damage, or intent.[145] Bruce Sterling succinctly explains the implications of this argument by observing that, "police want to believe all hackers are thieves."[146] If one believes all computer intruders possess a significant, if not equivalent, degree of culpability, in a situation of limited resources it is logical to prioritize cases by the ease of apprehension. Consequently, resources are shifted towards pursuing the criminals that are easiest to catch, namely script-kiddies. Compounding this problem is a lack of technological sophistication on the part of criminal justice professionals. Although the focus on computer crime continues to intensify and more specialists are being committed to this area, the general level of computing knowledge remains very low.[147] The difference between kingpins and mules in the computer crime taxonomy may not be immediately apparent to a federal prosecutor, making a low-level offender focus all the more likely.

C. Retribution and the Morality of Punishing Cybercrime

The other possible justification for severe penalties for computer crime is retribution, punishing behavior that offends societal norms. Although there are different theories of retribution, one common principle they share is proportionality: the punishment exacted must approximate the harm perpetrated.[148] Computer crime is nonviolent and results only in economic harm. Therefore, a victim corporation could be made whole by seeking a remedy in tort law or under the civil liability subsection of the CFAA. However, this Article does not contend that proportionality demands cybercriminals be exempt from criminal punishment or even incarceration. The harm from a computer attack can go beyond the victim corporation, as

---

145. *Id*.

146. STERLING, *supra* note 65, at 63.

147. Goodman, *supra* note 143, at 479-80 (focusing on police officers, but utilizing studies that are indicate an overall lack of knowledge); Wall, *supra* note 143, at 211.

148. Philosophical support for proportionality can be traced back to Immanuel Kant and his critique of utilitarian approaches to punishment. The crux of his position is that no benefit accruing to the criminal or society will justify punishment that is not otherwise necessary to maintain the moral equilibrium. IMMANUEL KANT, NETAPHYSICS OF MORALS 141 (Mary Gregor trans., Cambridge University Press 1991) (1797). More contemporary support can be found in the theories of Andrew von Hirsch, Michael Walzer, and John Rawls. *See, e.g.*, ANDREW VON HIRSCH, DOING JUSTICE: THE CHOICE OF PUNISHMENTS 67-76 (1976); MICHAEL WALZER, JUST AND UNJUST WARS: A MORAL ARGUMENT WITH HISTORICAL ILLUSTRATIONS (2000); John Rawls, *Two Concepts of Rules*, 64 PHIL. REV. 3, 4-5 (1955).

the damage could have severe effects for stockholders and the economy in general. There may also be indirect consequences. Attacks can create a climate of fear that can stifle online commerce or cause companies to inefficiently over-invest in security. Additionally, cybercriminals generally do not have sufficient funds to repay those they injure, making civil remedies insufficient for providing proper punishment.

While there is a general moral case for strong penalties, some countervailing factors call into question whether the current level of punishment is too high. It may be improper to assign complete moral culpability for the damage from computer attacks to cybercriminals. As was explained earlier, many companies purposely choose to under-invest in computer security and others negligently fail to repair widely known holes in their networks. Duff and Gardiner note that European law recognizes a duty on the part of the data holder to take sufficient security measures to protect its data.[149] They contend that holding the computer hacker fully culpable for economic damage when a company has been derelict with respect to this duty is not just.[150] Although no analogous affirmative duty exists in the United States, their argument is still forceful at a philosophical level. Admittedly, a problem for this position is that hackers have freely chosen to exploit these security holes. However, Duff and Gardiner's point is supported by the fact that a significant portion of the costs from a given attack are not directly attributable to the computer criminal. The high expense of resecuring results from the need to fix any security holes that existed prior to the attacker's action. Furthermore, the damage to a company's reputation comes from the public perception that the company is negligent with regard to security and is vulnerable to further attacks, both of which are probably accurate. Hackers do not choose targets at random and, to a large degree, they do not have sufficient skill to penetrate adequately secure systems. Similar to how truth is always a defense against a libel claim, it is wrong to blame hackers for simply revealing the innate weaknesses of a company's security implementation.

Removing resecuring costs and lost customer goodwill from the damage calculation makes it far more difficult to justify harsh penalties on retributive grounds. Without these tangential harms, the damage from most attacks is fairly localized and does not justify the penalties that exist under the USAPA. Intentional cracking that causes significant financial losses

149. Duff & Gardiner, *supra* note 137, at 220-21; *see also* Chris Pounder, *The Emergence of a Comprehensive Obligation Towards Computer Security*, 21 COMPUTERS & SEC. 328, 328-9 (2002) (explaining the obligations of data controllers under both UK and EU statutes).

150. Duff & Gardiner, *supra* note 137, at 221.

should still be severely punished, but this would be possible under a CFAA with a different structure.

VII. A WAY FORWARD

In the past twenty-five years we have witnessed a revolution in computing that first brought the computer into the home and then connected it to the world. Twenty-five years is a relatively brief time period for such dramatic technological change and society is still grappling with related social issues like computer hacking. Lawrence Lessig provides an excellent summary of how society has decided to make sense of hacking, and respond to it:

> It didn't take much to see that this world would not survive for long. This community of people who thought it fair to test the locks, enter someone else's machine if they could, and snoop their file structure—this community was not going to mesh with a Net where commerce could survive. It may have been fine to play these games in a world of geeks, but when money came online a better system of security was inevitable.
>
> As these cultures came into conflict, real-space law quickly took sides. Law worked ruthlessly to kill a certain kind of online community. The law made the hackers' behavior a "crime," and the government took aggressive steps to combat it. A few prominent and well-publicized cases were used to redefine the hackers' "harmless behavior" into what the law would call "criminal." The law thus erased any ambiguity about the "good" in hacking.[151]

This Article is not responding to the criminalization of hacking, as defined by Lessig, but to the mindset with which it has been done. Lessig's words effectively capture the reactionary nature of the governmental response, how the foreignness of the threat was dealt with by simplistically defining computer hacking as unequivocally criminal. In 1986, the economic potential of online commerce was not yet apparent, and Congress was able to consider rationally how to balance the various issues involved without fear of alienating business interests. The result was a sensible piece of legislation built upon the distinction between computer trespass and harmful computer crime, and now it is time to revise the CFAA to resurrect this distinction.

---

151. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 194 (1999).

Such a revision could take many forms, but there are a number of changes that are particularly important. The felony monetary threshold should be increased to $10,000, with resecuring costs exempted. Reputational damage should also be exempted, unless it could be shown that the damage was caused intentionally and was a foreseeable consequence of the attack. The requisite intent for each section of the Act must also be clarified. In particular, the difference between recklessness and negligence for the purposes of subsection (a)(5) should be expounded. Such an explanation would aid those courts that might not be well-versed in technological issues and give script-kiddies, hackers, and crackers alike the fair warning that they deserve. Additionally, *Czubinski*'s "idle curiosity" distinction should be codified into law as part of the (a)(4) fraud subsection in order to ensure that those fraud provisions are only applied to situations where there is a genuine illicit purpose. Finally, the USAPA sentencing changes should not be implemented until more is known about the deterrent effect of computer crime penalties and, even then, the Sentencing Commission should be instructed to adjust the Guidelines for the purposes of moderating the use of these long sentences. These changes, and others like them, can help ensure that the CFAA is an effective and balanced instrument in promoting computer and network security.