Loyola University Chicago Law Journal

Volume 35
Issue 1 *Fall 2003*

Article 9

2003

Mixed Metaphors in Cyberspace: Property in Information and Information Systems

Jacqueline Lipton
Case Western Reserve University School of Law

Mixed Metaphors in Cyberspace: Property in Information and Information Systems

*Jacqueline Lipton**

TABLE OF CONTENTS

I. INTRODUCTION

An essential truth has to be acknowledged—a computer cannot function without data. Data constitutes both the information stored within a computer and the programming instructions that allow a computer to function. Legislators have sought to criminalise damage to the storage device, to protect computer integrity rather than the data itself . . . . It is submitted that it is more appropriate to focus on what

* Assistant Professor, Case Western Reserve University School of Law, 11075 East Boulevard, Cleveland, OH 44106, (E-mail: jdl14@cwru.edu, Fax: (216) 368-2086), BA (Melb), BA (Hons) (La Trobe), LLB (Hons) (Melb), LLM (Monash), LLM (Cambridge), PhD (Griffith), Barrister and Solicitor of the Supreme Court of Victoria and the High Court of Australia. The author would like to thank Professor Jane Winn and others involved in the AALS Law and Computers Panel session in Washington DC in January 2003 for their comments on some aspects of the arguments presented in this Article. Alanna Arnold provided valuable research assistance.

> is actually being damaged, that being the data, than the box wherein it is contained.[1]

These words were written by a law student, Dane McLeod, who was commenting on recent Australian approaches to tortious and criminal offenses involving unauthorized access to or interference with a computer environment. McLeod's comments contain interesting and important observations that effectively illustrate the focus of much of this Article. In discussing the creation of legal prohibitions on certain conduct involving computers, McLeod criticizes the Australian approach for focusing on the physical aspects of the computer system, the "storage device" or "box," rather than what is actually of value within the system, the "data." This approach is also evident, to some extent, in other jurisdictions such as the United States.[2] However, the law in some other jurisdictions more clearly focuses on damage to data per se as opposed to damage to the "box" in which data might be stored.[3]

This Article utilizes a comparative case study to comment on the use of property metaphors in describing aspects of information and information systems in a legal and regulatory context. The relevant "metaphor" literature is connected to the issues raised above in the sense that the commentators on property metaphors in cyberspace point to the ever increasing tendency to treat "cyberspace" as a "place" as if it were akin to real property.[4] Even where a "personal property" metaphor is expressly used[5] to describe cyberspace, aspects of real

---

1. Dane McLeod, *Regulating Damage on the Internet: A Tortious Approach?*, 27 MONASH U. L. REV. 344, 350 (2001) (arguing that recent approaches in Australia to drafting tort and criminal legislation regarding damage to information systems have incorrectly focused on the physical attributes of computer systems, rather than on the valuable data contained therein).

2. As the following discussion will demonstrate, in the United States there appears to have been some confusion, both in relation to the common-law chattel trespass action and the application of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2000), about whether the harm to the plaintiff/victim is harm to a computer system or to information stored within the system. *See* MARK LEMLEY ET AL., SOFTWARE AND INTERNET LAW 940–81 (2d ed. 2003) (discussing the various aspects of the law of trespass to chattels as it applies to computer systems and the application of the Computer Fraud and Abuse Act in the United States).

3. For example, the British Computer Misuse Act creates offenses relating to unauthorized accesses to, and uses of, material stored in computers, such as computer programs and computer data. Computer Misuse Act, 1990, c. 18, §§ 1–3 (Eng.).

4. Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439, 503 (2003); Maureen O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 BERKELEY TECH L.J. 561, 586 (2001). *See generally* Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521 (2003).

5. *See* eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1069–70 (N.D. Cal. 2000) (raising "chattel trespass" arguments in relation to computer systems based on personal property rights in servers).

property still seem to creep into the relevant discussions.[6] This potentially leads to the drafting and interpretation of laws premised on "real-place-like" concepts, such as trespass, rather than laws that focus on protecting the item of real value to the complainant: the data stored within a system.[7]

The following discussion provides a basic critique of the use of property metaphors in cyberspace. It employs a case study on American and European Union laws relating to "bad faith," or unauthorized, accesses to and uses of "proprietary" information stored within information systems. The fundamental points argued are set out as follows:

(A) It is impossible to avoid the use of property metaphors in cyberspace.[8] However, such metaphors should be used with care. Real property metaphors should be avoided altogether.[9] Personal property metaphors are appropriate both to describe the physical hardware aspects of computer systems, which are incontrovertibly a species of tangible personal property, and also to describe the information/data contained within the systems, a proposition that some may find more controversial.[10]

(B) Once we accept the personal property label for both physical computer systems and information/data, it is necessary to decide just what aspects of cyberspace should appropriately be regulated. There

---

6. *See* Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 28–32 (2000) (noting the confusion between real and personal property analogies in deciding computer trespass cases); *see also* LEMLEY ET AL., *supra* note 2, at 948; Hunter, *supra* note 4, at 503.

7. McLeod, *supra* note 1, at 350.

8. Hunter, *supra* note 4, at 444 (suggesting that the property metaphor is very powerful as a matter of human cognition).

9. *Id.* at 516; Lemley, *supra* note 4, at 540.

10. There is a growing body of literature in which concerns have been expressed about the law's tendency to "over-propertize" information and information products. *E.g.*, Mark A. Lemley, *Private Property*, 52 STAN. L. REV. 1545 (2000) (examining arguments for and against treating personal information as property); Jacqueline Lipton, *Information Wants To Be Property: Legal Commodification of E-Commerce Assets*, 16 INT'L REV. L. COMP. & TECH. 53 (2002) (examining moves in a number of jurisdictions toward the increasing propertization of information products); 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 (2001) (discussing concerns that the Digital Millennium Copyright Act ("DMCA") will over-propertize digital information if courts do not take an adequate stance on protecting fair uses). *But see* Anupam Chander, *The New, New Property*, 81 TEX. L. REV. 715, 778–79 (2003) (suggesting that it may not be propertization per se that is the problem but rather the way in which property rights are utilized and regulated in the digital economy). *See generally* J.H. Reichman & Pamela Samuelson, *Intellectual Property Rights in Data?*, 50 VAND. L. REV. 51 (1997) (discussing the concerns about creating powerful property rights in databases in the United States).

may be a place for regulating conduct harmful to physical computer systems, but what is probably of greater importance and concern is creating a sensible approach to regulating unauthorized bad faith conduct involving digital data.

(C) It is therefore necessary to decide, both domestically and globally, what types of conduct in relation to such data should be proscribed, and how those proscriptions might be enforced effectively. Some possible approaches to these issues are suggested below.

Part II briefly surveys concerns about the use of property metaphors in cyberspace and explains why the use of personal property (information-as-thing)[11] metaphors cannot, and indeed need not, be avoided in cyberspace. Digital data is the item of paramount importance to those operating online businesses. The appropriate focus of any information/information technology law should be on protecting rights in this data or information, as distinct from rights in computer systems in which data or information might be stored or through which it might be transmitted.

Part III identifies the conduct that might be proscribed by law in relation to such data. Those who hold proprietary interests in data are concerned primarily with four possible unauthorized activities: (a) unauthorized access, (b) unauthorized use, (c) unauthorized damage/destruction, and (d) theft/misappropriation. A regulatory framework organized around these forms of conduct is most likely to achieve internal consistency and meet the needs of those who hold proprietary interests in information. Such an approach also potentially creates a roadmap for international harmonization in this area.

Part IV surveys the patchwork of laws currently applied to the regulation of valuable information stored electronically in light of the framework postulated in Part III. It compares and contrasts the position in the United States with that in the European Union to demonstrate that these laws are not only internally incoherent but also are not harmonized amongst different jurisdictions. This is likely to become a significant problem in an increasingly global society.

Finally, Part V suggests some directions for future action both domestically and internationally. The focus here is on the kinds of questions lawmakers and policymakers should ask to develop appropriate approaches to regulation of data and information systems in the information age.

---

11. Michael J. Madison, *Rights of Access and the Shape of the Internet*, 44 B.C. L. REV. 433, 442–46 (2003) (distinguishing the information as thing metaphor from the cyberspace as place metaphor).

Clearly much is premised here on the assumption that property rights in valuable information/data are desirable and should be protected by law. This is a contentious point of view, given the amount of literature currently arguing against expansive property rights in information and ideas.[12] As will become apparent from the following discussion, my own personal stance is that property rights in information are not necessarily to be avoided if they are monitored appropriately and controlled by the governments that create them.[13] Such monitoring and control can be achieved in a variety of ways. This is an issue I have canvassed elsewhere and will not be arguing in any detail here.[14]

I mention it, however, because it is fundamental to understanding why I advocate property rights in information, and because it is important to point out that I am not suggesting the adoption of wholesale unfettered property rights that potentially lead to large-scale monopolies of information. I share the concerns of the commentators who have criticized the disturbing trend by governments to "over-propertize" information in the digital age.[15] My arguments are premised on the assumption that governments the world over should start taking a more balanced view in relation to the regulation of information property rights than they have in the past;[16] indeed, governments should take a more active role in monitoring and limiting commercial exploitation of those rights. I argue that this can be

12. *See supra* note 10 (citing a sampling of the relevant literature critiquing property rights in intellectual property).

13. I have argued this previously in relation to property rights in electronic databases. Jacqueline Lipton, *Balancing Private Rights and Public Policies: Reconceptualizing Property in Databases*, 18 BERKELEY TECH. L.J. 773 (2003) [hereinafter Lipton, *Balancing Private Rights*] (describing ways in which a government can effectively control and monitor any property rights it grants in electronic databases).

14. *Id.*; *see also* Chander, *supra* note 10, at 778–80 (arguing that property rights in domain names, like rights in other forms of property, would not result in absolute dominion and can be limited by law); Jacqueline Lipton, *A Framework for Information Law and Policy*, 82 OR. L. REV. (forthcoming 2004) (manuscript on file with author) [hereinafter Lipton, *Framework*] (arguing that it is possible to juxtapose various public and private rights in information to achieve an appropriate policy balance even where extensive information property rights are accepted as a matter of law); Jacqueline Lipton, *Information Property: Rights and Responsibilities*, 55 FLA. L. REV. (forthcoming 2003) (manuscript on file with author) [hereinafter Lipton, *Rights and Responsibilities*].

15. *See supra* note 10 and accompanying text (discussing "over-propertization" in the information technology setting).

16. Lipton, *Balancing Private Rights*, *supra* note 13, at 778–79; Lipton, *Rights and Responsibilities*, *supra* note 14.

achieved by utilizing the personal property concept as a tool to create a balance between public and private interests in information.[17]

The following discussion focuses on unauthorized incursions, usually committed by competitors or those who might seek to damage the commercial reputation and/or potential of an online business. My suggestions are premised on the idea that "unauthorized" in this context describes those who *intentionally seek to damage* the commercial or economic interests of the possessor of the information.

Legal issues relating to good faith accesses and uses of information for public purposes, such as scientific and educational purposes, are not covered here.[18] These are undoubtedly very important issues and to some extent they cannot really be divorced from the issues addressed in this Article, as evidenced in the concluding sections of this discussion. Nonetheless, the aim of this Article is to focus on the types of conduct that a holder of proprietary information might reasonably complain about, and for which legal redress should be available.

II. MIXED METAPHORS IN CYBERSPACE

A. Real Property Versus Personal Property Metaphors

This discussion starts with one basic proposition: regardless of what anyone has said about the undesirability of incorporating notions of property into information and information systems,[19] there is no practical way to avoid this outcome. In dealing with any new issue that raises legal problems, the human mind will tend to use familiar concepts to explain and organize the unfamiliar.[20] There are, in fact, distinct

17. Lipton, *Balancing Private Rights*, *supra* note 13, at 776; Lipton, *Rights and Responsibilities*, *supra* note 14.

18. There is much literature about the need to preserve what I would term "good faith" uses of information, including scientific and educational purposes. *E.g.*, David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 702 (2000) (arguing that there is a need to preserve fair use exceptions to copyright infringement in the digital age); *see also, e.g.*, 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, 831–32 (1999) (discussing the need to preserve scientific and technological uses of information in the wake of the creation of property rights in databases). *See generally* 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 (1999) (asserting the fair use doctrine in the digital age should be preserved).

19. *See supra* note 10 (positing the various undesirable manifestations of using property notions in information technology settings).

20. Hunter, *supra* note 4, at 444; Madison, *supra* note 11, at 439.

advantages to doing so.[21] Familiar labels and metaphors can provide effective and efficient shorthand methods for describing and organizing new things, and can demonstrate how we, as members of a given society at a given time, feel about a particular new issue.[22]

What is important in the age of information technology is not *whether* we use property metaphors to describe and organize laws, but *how* we use those metaphors. Arguably, one of the problems with property metaphors in cyberspace in the past, including the cyberspace metaphor itself, is the confused way in which they have been used. Metaphors can be useful tools to simplify a new and complex problem.[23] Yet, in the context of information and information technology, property metaphors have been used inconsistently and imprecisely by courts and commentators, leading to some confusion about the types of legal rights being created in relevant aspects of information technology.

As an example, and to echo McLeod's concerns,[24] in cases where plaintiffs have been concerned about chattel trespass in relation to their computer systems, connoting a personal property right in the system (or in electrons flowing through the system),[25] plaintiffs have in fact assumed that they have real-property-like rights in computer systems.[26] This has led to courts taking inconsistent views about property rights in information systems. All of the physical aspects of information systems—hardware, cabling, physical storage devices, and probably also electrons flowing through the system—may be regarded as personal property, but they are clearly not real property. Any actual interference with these items might give rise to a chattel trespass claim, if the elements of that claim are made out.

Trespass to chattels is a common law tort that deals with unauthorized use of or intermeddling with another's personal

21. *See* Alfred C. Yen, *Western Frontier or Feudal Society?: Metaphors and Perceptions of Cyberspace*, 17 BERKELEY TECH. L.J. 1207, 1209 (2003) (demonstrating how different property metaphors can help inform regulatory developments in cyberspace).

22. Hunter, *supra* note 4, at 444; Madison, *supra* note 11, at 439; Yen, *supra* note 21, at 1209.

23. Hunter, *supra* note 4, at 444; Madison, *supra* note 11, at 439; Yen, *supra* note 21, at 1209.

24. *See supra* note 1 and accompanying text (discussing Australia's approach in drafting tort legislation in response to information tampering).

25. CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (acknowledging that "[e]lectronic signals generated and sent by computer have been held to be sufficiently physically tangible to support a trespass cause of action").

26. Hunter, *supra* note 4, at 443.

property.[27] The elements of the tort require that the interference (a) be intentional, (b) be unauthorized, (c) be substantial, (d) involve actual harm or serious infringement of rights, and (e) involve physical contact with the property in question.[28] The tort will only apply to physical, tangible personal property, as distinct from real property and intangible intellectual property.[29]

Thus, a claim for chattel trespass obviously could be made with respect to actual physical interference with the hardware aspects of a computer system. However, the circumstances would have to involve impairment of the condition, quality, or value of the hardware,[30] or deprivation of the use of the hardware for a substantial period of time.[31] This would appear to limit the operation of the tort to cases of physical vandalism. Even if electrons are regarded as tangible, physical property, it is hard to imagine substantial interference with electrons that causes such a result in practice.

Nevertheless, some courts have found chattel trespass claims in relation to computer systems on the basis of relatively minor amounts of interference, including electrons flowing through a system and inconvenience to a plaintiff's customers from unwanted spam.[32] In most of these cases, plaintiffs have been concerned in reality with defendants making unauthorized incursions into plaintiffs' systems to gain some kind of commercial advantage. Examples include situations where a defendant makes unauthorized use of information stored within a plaintiff's system, such as customer details for targeted marketing purposes, or information on the plaintiff's available products and services for market research and/or Web aggregation purposes.[33]

---

27. RESTATEMENT (SECOND) OF TORTS § 217 (1965); *see also* America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 451–52 (E.D. Va. 1998); R. Clifton Merrel, *Trespass to Chattels in the Age of the Internet*, 80 WASH. U. L.Q. 675, 677–78 (2002).

28. RESTATEMENT (SECOND) OF TORTS § 218(b); Laura Quilter, Briefing Paper, Trespass to Chattel Doctrine Applied to Cyberspace 1 (2001) (unpublished manuscript, on file with author), *available at* http://www.law.berkeley.edu/institutes/bclt/pubs/annrev/exmplrs/bp/lqbp.pdf (last visited Oct. 22, 2003).

29. RESTATEMENT (SECOND) OF TORTS § 218(b); *see also* Edward W. Chang, *Bidding on Trespass:* eBay, Inc. v. Bidder's Edge, Inc. *and the Abuse of Trespass Theory in Cyberspace-law*, 29 AIPLA Q.J. 445, 447 (2001); Quilter, *supra* note 28, at 1.

30. RESTATEMENT (SECOND) OF TORTS § 218(b).

31. *Id.*

32. CompuServe Inc., v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1022 (S.D. Ohio 1997). *But see* LEMLEY ET AL., *supra* note 2, at 948 (querying whether this analysis makes sense in practice).

33. HONGWEI ZHU ET AL., THE INTERPLAY OF WEB AGGREGATION AND REGULATIONS § 2.1 (MIT Sloan Sch. of Mgmt., Working Paper No. 4397-02, 2002) (describing the legal and

If a plaintiff is truly concerned with a defendant making unauthorized uses of his or her valuable information, the problem does not necessarily arise from the fact that the plaintiff feels that he or she "owns" the website. Rather, it arises from the fact that the law has not developed sufficiently tailored responses to problems involving unauthorized uses of valuable information about which the plaintiff may feel equally proprietarial. To alleviate these concerns, judges might bend and stretch existing chattel trespass laws to the breaking point to protect the information under the guise of protecting the sanctity of the website, as if it were a real place.[34]

Many of those who have criticized the use of property metaphors underlying the application of the chattel trespass doctrine in the information technology context are not so concerned about the *fact* that the metaphors are used, but rather about *how* those metaphors are employed. If litigants and courts had made more *consistent* and *precise* uses of property metaphors here, and if chattel trespass claims were litigated with strict adherence to their constituent elements, the use of the term "property" in this context would be much less controversial.

Obviously the above oversimplifies the issue somewhat; the real problems are a little more complex than suggested here. For one thing, common-law computer trespass is not the most troubling example of the use of property metaphors in the information age, although it does exemplify one of the most inconsistent areas of application of law by courts. Many scholars have been much more concerned about, say, developments in copyright law that bolster the proprietary quality of information stored in computer systems[35] or developments in sui generis database law in the European Union.[36] However, these examples are really more about the information-as-thing[37] metaphor

technological aspects of web aggregation services), *available at* http://ssrn.com/abstract_id=365061 (last visited Oct. 23, 2003).

34. eBay, Inc. v Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1069–70 (N.D. Cal. 2000); Quilter, *supra* note 28, at 5–6.

35. Nimmer, *supra* note 18, at 683; Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need To Be Revised*, 14 BERKELEY TECH. L.J. 519, 521–22 (1999).

36. Council Directive 96/9/EC of 11 March 1996 on the Legal Protection of Databases, 1996 O.J. (L 77) [hereinafter E.U. Database Directive], *available at* http://europa.eu.int (last visited Oct. 25, 2003).

37. Madison, *supra* note 11, at 446–47 (describing the difference between information as thing and cyberspace as place metaphors).

than the cyberspace as place metaphor.[38] Before considering the former, it is desirable to dispense with the latter.

I chose to commence with the computer trespass example because, in my view, it is important to start a discussion on the unpacking of these concepts in the information age with a basic example of how the confusion between real and personal property rights in information and information systems arises, so that the real property metaphor can be firmly set aside. It should satisfy the proprietary impulses of website operators if they are able to assert *personal* property rights in their computer hardware and website contents, provided that any such rights are appropriately tailored to the overall needs of the global information society in terms of access to and use of information.

Assuming the exclusion of the real property metaphor for all things cyber, we are then left with the question of how to use the personal property metaphor with respect to information and information technology. No one would doubt that physical aspects of a computer system can be personal property; they are just another example of a class of tangible objects that can be physically possessed. The more vexing question is whether information/data per se should be regarded as a species of personal property.

B. Personal Property in Cyberspace: The Data or the Box?

It is now time to turn this discussion back to the passage quoted at the beginning of this Article: McLeod's assertion that the Australian legislature has been missing the forest for the trees by focusing regulation on computer systems, the boxes or storage devices, rather than on data or information per se. It seems that there is some merit in maintaining a clear distinction between the box and the data stored in the box. There is currently confusion in many jurisdictions about the difference between focusing laws on protecting boxes, on the one hand, and data stored within the boxes on the other.[39]

Many instances of complaints about unauthorized access to a *computer system* are really premised on the complainant's concerns about unauthorized access to and/or use of data stored within the

38. *Id.* *But see* Hunter, *supra* note 4, at 446–47 ("[L]et me go further and suggest that all legislators, judges and lawyers unconsciously think that cyberspace is a place, even though at times they may argue vehemently that it is not.").

39. *See supra* note 2. Even in jurisdictions where laws are predominantly focused on protecting data within systems, such as the United Kingdom, there is some confusion about the boundaries of the legal framework within which this goal is to be realized. The following discussion considers this issue in more detail.

system.[40] This is another reason why real property metaphors in cyberspace should be avoided. Where a complainant's concern is really with unauthorized activities involving its proprietary data, the use of real property metaphors in relation to its computer system clearly misleads and does not deal directly with the issue at hand.

There may indeed be some situations in which website operators and Internet businesses have legitimate concerns about damage to *systems* per se. However, these situations do not merit a real property analysis. Examples might include: (a) distributed denial-of-service attacks;[41] (b) the creation and distribution of computer viruses;[42] (c) the use of web crawling "bots"[43] to aggregate information from a variety of websites to provide information to the public comparing, for example, prices available for particular products on those sites;[44] and (d) the growing problem of spam e-mails.[45]

As will be demonstrated in the following discussion, although these activities initially appear to relate to unauthorized access and use of websites as distinct from their contents, ultimately most of these examples implicate unauthorized conduct involving contents. In any event, all of these activities might be annoying, and some of them might

40. McLeod, *supra* note 1, at 50–51.

41. Distributed denial-of-service ("DDoS") attacks involve unauthorized intruders commandeering the computers of unsuspecting users and using these distributed systems, referred to as "zombies," to flood a particular website or service provider with junk messages. These messages will overwhelm the victim's servers and cause the website to deny service to its legitimate customers for a period of time. *See* Stephen E. Henderson & Matthew E. Yarbrough, *Suing the Insecure?: A Duty of Care in Cyberspace*, 32 N.M. L. REV. 11, 11 (2002) (stating that the "Internet can be crippled by distributed denial-of-service attacks launched by relatively unsophisticated and judgment proof parties"); Margaret Radin, *Distributed Denial of Service Attacks: Who Pays? (Part I)*, 6(9) CYBERSPACE LAW. 2 (2001).

42. Viruses are small pieces of software programming that piggyback onto real programs. They run every time the real program runs and reproduce by attaching to other programs, wreaking havoc in the infected system generally. E-mail viruses replicate by automatically mailing themselves to dozens of people in a victim's e-mail address book. *See* HOWSTUFFWORKS, INC., HOW COMPUTER VIRUSES WORK, *at* http://computer.howstuffworks.com/virus.htm (last visited Sept. 27, 2003) [hereinafter HOWSTUFFWORKS] (describing the process by which a computer virus spreads); Yaman Akdeniz, *Section 3 of the Computer Misuse Act 1990: An Antidote for Computer Viruses!*, 3 WEB J. CURRENT LEGAL ISSUES, *at* http://webjcli.ncl.ac.uk/1996/issue3/akdeniz3.html (1996) (discussing the United Kingdom legislation on computer misuse).

43. eBay, Inc. v Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1061–62 (N.D. Cal. 2000) (discussing a defendant who was using "bots" to aggregate information from various online auction houses, including plaintiff's website); ZHU ET AL., *supra* note 33, § 3.2.

44. *eBay, Inc.*, 100 F. Supp. 2d at 1061–62; ZHU ET AL., *supra* note 33, § 3.

45. LEMLEY ET AL., *supra* note 2, at 921–40 (surveying relevant case law and legislative responses to the increasing problem of spam e-mails).

interfere with an online business' ability to serve its customers.[46] However, it is not clear that the law should proscribe all of them per se beyond the extent to which they might result in unauthorized access or damage to data.[47]

The immediately obvious items of value to online businesses are their information products, rather than their physical storage devices or even (generically) their websites per se. The items of value include (a) proprietary software; (b) databases of buyers, suppliers, customers, products, etc.; (c) trademark rights in names, logos, etc., utilized by the business; (d) Internet domain names; (e) business methods, trade secrets, know-how, etc.; and (f) website design or layout. Many of them already attract some form of intellectual property protection; for example, proprietary software will attract copyright protection[48] and, in some instances, will be patentable.[49] Internet domain names usually correspond to a trademark right and thus are protected ultimately by the trademark system.[50] Many aspects of electronic databases will be protected by copyright law,[51] although the actual database

46. For example, in a DDoS attack, the attack might cause the victim's system to crash for a period of time, thus preventing the website operator from providing service to its customers. Henderson & Yarbrough, *supra* note 41, at 11; Radin, *supra* note 41.

47. RONALD MANN & JANE WINN, ELECTRONIC COMMERCE 75–76 (2002) (discussing the possibility of establishing industry standards and practices for computer security rather than purely relying on legal liability for computer hacking); Mary M. Calkins, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171, 188–224 (2000) (analyzing various private and public models for preventing unauthorized computer hacking conduct, including the setting of government standards for computer security and government-funded education programs to support the standards, rather than relying purely on legal liability for hacking).

48. LEMLEY ET AL., *supra* note 2, at 33–94 (detailing the basis upon which various aspects of software have attracted copyright protection).

49. Patent protection for software was originally a somewhat vexing question. There were strong arguments made against granting software patents. *E.g.*, John Swinson, *Copyright or Patent or Both? An Algorithmic Approach to Computer Software Protection*, 5 HARV. J.L. & TECH. 145, 146 (1991); John Swinson, *Software Patents in the United States*, 4 J.L. & INFO. SCI. 116, 124–41 (1993). However, over the years, software patents have increasingly been accepted in the United States, and many commentators advocate their use. *See, e.g.*, Julie Cohen & Mark Lemley, *Patent Scope and Innovation in the Software Industry*, 89 CAL. L. REV. 1, 4 (2001).

50. Certainly, the Uniform Domain-Name Dispute-Resolution Policy ("UDRP") implemented by the Internet Corporation for Assigned Names and Numbers ("ICANN") relies on the relationship between domain names and trademarks in ascertaining the difference between good faith and bad faith domain-name registrations. THE INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS, UNIFORM DOMAIN-NAME DISPUTE-RESOLUTION POLICY para. 4(a)(i), (b)(i)–(ii), (iv), *at* http://www.icann.org/dndr/udrp/policy.htm (Oct. 24, 1999).

51. Any original software utilized in the database, such as the search engine program, will be copyrightable as a literary work. Mary M. Brown et al., *Database Protection in a Digital World*, 6 RICH. J.L. & TECH. 2, para. 62, *at* http://law.richmond.edu/jolt/v6i1/conley.html (1999). The visual format of the results may also be patentable as an artistic or graphical work. *Id.*

contents will not be protected as such, at least in the United States.[52]

The main problem with these existing intellectual property rights in the context under discussion here is that they have not been created as part of a cohesive policy framework for information law,[53] and they are not internationally harmonized, as the following discussion will demonstrate. However, such property rights can be useful if appropriately organized.

C. The Impetus for Information Property Rights

A personal property concept in information may be particularly useful if tailored appropriately to meet competing needs for rights in information generally. The personal property concept has proved useful in the past in relation to items that have some commercial value and in which parties desire to trade.[54] Property is obviously a complex concept and it connotes many things. However, the practical impetus for describing something as property, rather than adopting some other characterization, usually comes down to a need to trade in the item. It tends to be driven by those who seek to develop a market relating to a specific item. The law then follows the market by creating and supporting the property right in question, either by statute,[55]

52. Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 361–62 (1991) (holding that to meet the originality standard for copyright protection a database or compilation needed to show sufficient originality in the selection or arrangement of its contents). Mere "sweat of the brow" in compiling a database would be insufficient to attract copyright protection. *Id.* at 353. The E.U. Database Directive takes a different approach, as outlined below. *See infra* notes 142–148 and accompanying text (describing database protection in the European Union).

53. I have argued elsewhere that it may now be time to think about creating a broader information law and policy framework for the global information age. Lipton, *Framework*, *supra* note 14.

54. *See* Radhika Rao, *Property, Privacy, and the Human Body*, 80 B.U. L. REV. 359, 364 (2000) (noting that the difference between a *privacy* right in elements of the human body and a *property* right lies in the impetus for trade connoted by the property right); *see also* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1295–97 (2000) (making similar observations in the information property context).

55. In fact, this is how intellectual property rights were created in the first place, by following the perceived requirements of the market to encourage innovation. *See* Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 558 (1985); Steve P. Calandrillo, *An Economic Analysis of Intellectual Property Rights: Justifications and Problems of Exclusive Rights, Incentives To Generate Information, and the Alternative of a Government-run Reward System*, 9 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 301, 304–05 (1998) (discussing economic considerations of copyright and patent law).

through the courts,[56] or both.[57] Professor Litman has noted, "[t]he *raison d'etre* of property is alienability; the purpose of property laws is to prescribe the conditions for transfer. Property law gives owners control over an item and the ability to sell or license it."[58]

With respect to intellectual property rights generally, many commentators also have pointed to various utilitarian[59] and Lockean justifications[60] for the grant of such rights by legislatures.[61] In terms of utilitarian justifications, commentators often argue that, absent the grant of intellectual property rights, there would be insufficient incentives for people to create artistic and scientific works because of the non-rivalrous, public-goods[62] qualities of such works.

This does not contradict the above point about the impetus for the creation of property, as opposed to other forms of rights in information products. Obviously the types of rewards contemplated here are economic or commercial, meaning the ability to trade with the relevant

---

56. Int'l News Serv. v. Associated Press, 248 U.S. 215, 236–37 (1918) (creating a temporary "quasi property" right in non-copyrightable news reports).

57. Trade secrets have been recognized as property rights both in legislation and by the courts. Economic Espionage Act of 1996 § 101, 18 U.S.C. §§ 1831–1839 (2000), *amended by* Criminal Law Technical Amendments Act of 2002, Pub. L. No. 107-273, § 4002(e)(9), 116 Stat. 1806, 1810; Ruckleshaus v. Monsanto Co., 467 U.S. 986, 1003–04 (1984).

58. Litman, *supra* note 54, at 1295.

59. See Andrew Beckerman-Rodau, *Are Ideas Within the Traditional Definition of Property?: A Jurisprudential Analysis*, 47 ARK. L. REV. 603, 612–13 (1994) (discussing the utilitarian justification for intellectual property); Edwin C. Hettinger, *Justifying Intellectual Property*, 18 PHIL. & PUB. AFFAIRS 31, 47–50 (1989) (containing utilitarian arguments supporting the grant of intellectual property rights); Tom G. Palmer, *Are Patents and Copyrights Morally Justified? The Philosophy of Property Rights and Ideal Objects*, 13 HARV. J.L. & PUB. POL'Y 817, 820 (1990) (noting that utilitarian arguments can both support and refute the need for intellectual property).

60. Justin Hughes, *The Philosophy of Intellectual Property*, 77 GEO. L.J. 287, 297–330 (1988) (analyzing Lockean justifications for intellectual property rights); Adam D. Moore, *A Lockean Theory of Intellectual Property*, 21 HAMLINE L. REV. 65, 66 (1997).

61. Other theories have also been used to explain grants of intellectual property rights. *See* Wendy J. Gordon, *A Property Right in Self-expression: Equality and Individualism in the Natural Law of Intellectual Property*, 102 YALE L.J. 1533, 1540–1606 (1993) (outlining natural law theory of intellectual property rights and the relationship of the right to self expression); Wendy J. Gordon, *On Owning Information: Intellectual Property and the Restitutionary Impulse*, 78 VA. L. REV. 149 (1992) (outlining a restitutionary model for intellectual property rights at the state level); Hughes, *supra* note 60, at 330–56 (outlining a Hegelian "personality" theory of intellectual property rights).

62. "Public goods" are those goods that can be shared non-rivalrously by many, and from whose use non-payers are not easily excluded. Wendy J. Gordon, *Authors, Publishers, and Public Goods: Trading Gold for Dross*, 36 LOY. L.A. L. REV. 159, 164 (2002). Inventions and works of authorship are public goods. *Id.* Their creation is economically stimulated by the limited private exclusion rights granted under patent and copyright laws. *Id.*; *see also* Wendy J. Gordon, *Asymmetric Market Failure and Prisoner's Dilemma in Intellectual Property*, 17 U. DAYTON L. REV. 853, 854 (1992) (discussing conditions where intellectual property rights are necessary to prevent market failure).

works in a market. Other forms of reward could have been contemplated by the legislature, such as public recognition for the creation of a scientific or artistic work.[63] These forms of reward presumably would not require a property right per se because they are not based on economic ideals and the need to encourage commerce with the works in question. However, even under such a model, it is likely that at some point someone, be it the creator of the works or someone else, would want to trade in the works, and a property right would need to be created to facilitate such trade.

Likewise with the Lockean justification for intellectual property rights, the basic idea is that people are entitled to enjoy the fruits of their labors.[64] One who makes the effort to appropriate something from the commons[65] is entitled to enjoy the benefit of that appropriation, provided that he leaves "as much and as good" for others[66] and does not waste the assets in question.[67] This theory obviously was not developed with intellectual property rights in mind, but often has been used to justify their grant.[68] The obvious assumption here is that there is a form of "intellectual commons" from which ideas can be appropriated.[69]

As with the utilitarian justification, the benefit granted to the appropriator under the Lockean analysis takes the form of a property right rather than some other form of right. Again, we can ask the question: Why does the right take a property form? Presumably, again, it forms at least partly because of the desire to trade in an object that has

---

63. In some ways, this is what moral rights law is about. The United States has very limited moral rights provisions in its copyright law. Visual Artists Rights Act of 1990 § 602, 17 U.S.C. § 101 (2000) (creating federal moral rights of attribution and integrity for artists in their work by recognizing an artist's legally protectable interests in claiming authorship of his or her work and in the physical integrity of his or her visual art, even after it is sold, for the lifetime of the artist or author). However, other jurisdictions, including the European Union and Australia, have more detailed moral rights provisions in their copyright laws. *See, e.g.*, Copyright, Designs and Patents Act, 1988, c.48, §§ 77–89 (Eng.); Copyright Act, 1968, §§ 189–195 (Austl.).

64. JOHN LOCKE, *The Second Treatise of Civil Government*, *in* TWO TREATISES OF CIVIL GOVERNMENT 121, paras. 27–30, at 134–36 (Thomas I. Cook ed., Hafner Publ'g Co. 1947) (1690).

65. *Id.* paras. 27, 32. Of course, the application of this idea to information property assumes that there is a kind of "intellectual commons." R. Anthony Reese, *Reflections on the Intellectual Commons: Two Perspectives on Copyright Duration and Reversion*, 47 STAN. L. REV. 707, 710–11 (1995).

66. LOCKE, *supra* note 64, para. 36.

67. *Id.* para. 33.

68. *See supra* note 60 (citing to works analyzing Lockean theories of intellectual property rights).

69. Michael J. Madison, *Legal-Ware: Contract and Copyright in the Digital Age*, 67 FORDHAM L. REV. 1025, 1097 (1998) (accepting the premise of an intellectual commons of information and ideas).

a market value. The property right can also exclude others from an item that a person has appropriated from the commons. Thus, the right serves an important exclusionary function. However, a privacy right might also serve such a function absent the desire to deal with the item in a market.[70] Thus, Professor Litman's assertion that property rights are created when alienability of an item is required seems to be borne out here.

Given that property rights appear to be particularly useful in the context of items with which people desire to trade in commerce, it seems inevitable that the types of information assets described above in relation to online businesses will ultimately attract a "property" label. Whether or not courts and legislatures expressly support such a model, market players will likely treat those items as property, unless the law expressly prohibits proprietary rights and trading in a particular item on public policy grounds.[71]

Even without a legal "property" label, the market can use other mechanisms such as contractual provisions and technological measures to achieve property-like ends.[72] Electronic databases are an obvious example of this. In the United States, databases that are insufficiently original in the selection or arrangement of their contents to attract copyright protection do not enjoy legal protection as the property of their compiler.[73] Even those databases that do attract copyright protection are only protected to the extent of their fixed literal expression.[74] There are no property rights in their contents.[75]

---

70. Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193, 198–99 (1890); *see also* Martin P. Hoffman, *The Rights of Publicity and Privacy*, *in* TRADEMARKS, COPYRIGHTS, AND UNFAIR COMPETITION FOR THE GENERAL PRACTITIONER 227, 229 (A.L.I.-A.B.A. Continuing Legal Educ., SB77, 1997) (discussing the historical basis for Brandeis and Warren's article).

71. For example, spleen cells and organs and other body parts, such as kidneys, livers, hearts, lungs, corneas, bone marrow, and skin cannot be sold as products, but can be donated. *See* Rao, *supra* note 54, at 373–74. Endangered species of animals and plants are protected through the regulation of hunting and trade in those species. *See* 22 U.S.C. § 2151(q) (2000).

72. William W. Fisher III, *Property and Contract on the Internet*, 73 CHI.-KENT L. REV. 1203, 1203 (1998); Madison, *supra* note 11, at 433–34.

73. Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 361–62 (1991).

74. *See* STEPHEN ELIAS, PATENT, COPYRIGHT & TRADEMARK: A DESK REFERENCE TO INTELLECTUAL PROPERTY LAW 66 (Lisa Goldoftas ed., Nolo Press 1996) (1941); John R. Dean, *The Sheriff Is Coming to Cyberville: Trademark and Copyright Law and the Internet*, 11 BYU J. PUB. L. 75, 96 (1997).

75. *See* ELIAS, *supra* note 74, at 66; Dean, *supra* note 74, at 96.

The fact that such databases-as-compilations are not regarded by U.S. law[76] as property does not stop those who compile them from trading in them.[77] Technological encryption measures are often utilized to prevent unauthorized access, and contractual licensing and transfer schemes are used for commercial transactions involving such databases.[78] Thus, the market effectively creates a property right where there is an impetus to deal commercially with the item in question, regardless of the stance a particular legislature might take on the creation of a property right.[79]

In this context, it is futile to argue that legislatures should not continue to create information property rights. What is more important is to recognize that the market drives, and will continue to drive, what is regarded as a property right. The appropriate role of the legislature should be to monitor and control the use of these rights.[80] This role will include ensuring that the rights do not: (a) encroach to an unjustifiable extent on the public domain of information and ideas;[81] (b) stifle invention, education, and creativity throughout society;[82] and (c) interfere with privacy interests in relation to personal information.[83]

Additionally, legislatures should identify precisely what forms of bad faith unauthorized conduct should be prohibited. It is to those issues that the remainder of this Article turns. I will present arguments in favor of creating a unified and cohesive framework for laws dealing

---

76. Not all jurisdictions follow this model. Australian copyright law does appear to allow copyright in an unoriginal database. Telstra Corp. v. Desktop Mktg. Sys. Pty Ltd. (2001) 51 I.P.R. 257 (allowing copyright protection for a white pages telephone book compiled electronically), *available at* http://www.austlii.edu.au/au/cases/cth/federal_ct/2001/612.html (last visited Sept. 27, 2003). This decision has been appealed unsuccessfully to the Full Court of the Federal Court of Australia and there is currently an appeal pending before the High Court of Australia. Desktop Mktg. Sys. Pty Ltd. v. Telstra Corp. (2002) 119 F.C.R. 491. The European Union has created a sui generis property right for unoriginal databases called the E.U. Database Directive. *See infra* notes 142–148 and accompanying text (describing database protection in the European Union).

77. For example, LEXIS, Westlaw, and Bureau for National Affairs (BNA) publications (legal research databases); Ancestry (fee-based online United States death indexes for genealogy searches); the Complete Marquis Who's Who (biographies database); DIALOG (leading supplier on online databases including DATASTAR, DialogWeb, and Profound); eLibrary (access to periodical database); and eMarketer (detailed market reports).

78. *See supra* note 77 (listing examples of various indices and databases).

79. As a result, I have argued elsewhere that it would be preferable for the United States Congress to accept property rights in electronic databases, but to closely monitor the commercial exploitation of such rights to prevent unjustified monopolies and to protect the public domain of information and ideas. Lipton, *Balancing Private Rights*, *supra* note 13, at 832–33.

80. *Id.*; Chander, *supra* note 10, at 771–72.

81. Lipton, *Balancing Private Rights*, *supra* note 13, at 781–82.

82. *Id.*

83. In respect of balancing property rights in information products against privacy rights in personal information, see Lipton, *Framework*, *supra* note 14.

with such bad faith unauthorized incursions into commercial information property rights. Any such framework should be based on the classes of conduct about which information owners are likely to be most concerned. These classes of conduct are identified in Part III. Part IV then examines how these issues are currently dealt with under a pastiche of laws both within the United States and throughout the European Union. Part V suggests ways in which these laws could be presented in terms of a more unified and harmonized theoretical framework.

III. DAMAGING DIGITAL DATA

Focusing now on the issue of how regulators should approach bad faith incursions into rights in proprietary information, the first step must be to identify the types of conduct with which they should be concerned. Laws and remedies crafted to support rights in *information* will be more likely to address the issues about which a complainant is actually concerned than the more indirect approach of basing legal sanctions on alleged damage to an information *system*. There will naturally be cases where a complainant is concerned about damage to an information system per se, but these are likely to be straightforward cases of criminal or tortious damage to the physical aspects of the system that will not require special new sui generis laws.

There are some more difficult cases where the physical attributes of a system are not damaged by a wrongdoer and where the information within the system is not necessarily damaged, but where the complainant's ability to effectively utilize its system or information contained therein is compromised. An obvious example of this is a distributed denial-of-service ("DDoS") attack. This involves unauthorized intruders commandeering the computers of unsuspecting users and using these distributed systems, referred to as "zombies," to flood a particular website or service provider with junk messages. These messages will overwhelm the victim's servers and will cause the website to deny service to its legitimate customers for a period of time.[84]

A DDoS attack does not necessarily involve damage to any physical system or to any information residing within a system, although it does interfere with a website operator's ability to provide service to its customers for a period of time. This may be a unique case requiring

84. Radin, *supra* note 41; *see also* Henderson & Yarbrough, *supra* note 41, at 11–14 (describing how DDoS attacks cripple computer systems).

specific legislative attention,[85] or it may be that such conduct should not attract a specific legal sanction where data is not actually damaged or destroyed as a result of the attack.

For the most part, however, activities that will be of particular concern to online businesses involve unauthorized interferences with their proprietary rights in information. Even the activities involving computer viruses or Web aggregation services, referred to in Part I,[86] can be explained in terms of concerns by the complainant about unauthorized damage to, access to, and/or distribution of information contained on its website or within its system. Viruses often damage or destroy data within a system or copy and forward such information to other systems.[87] Web aggregators take information from a website and re-present it in a comparative form on another website.[88] This may not involve unauthorized access to the information in the first place but could involve unauthorized use and distribution of the information.

Assuming, then, that the focus of any law aimed at protecting proprietary information against bad faith incursions should be focused on the impact of a wrongdoer's conduct on the information per se, the next step is to identify the types of impacts that should be prohibited. Most, if not all, bad faith activity in relation to information breaks down into at least one of four possible categories: (a) unauthorized access to the information; (b) unauthorized use, including copying and disclosure, of the information, regardless of whether or not the initial access was authorized; (c) damage to, or destruction of, the information; and (d) theft or misappropriation of the information.

These four categories of conduct in relation to information seem to sum up the concerns of information proprietors in the digital age. They are not necessarily mutually exclusive; for example, one cannot make an unauthorized *use* of proprietary information unless one has first *accessed* the information, although in any given case access may be authorized while subsequent use is not. There is also obviously a close relationship between access and misappropriation. In some circumstances, such as misappropriation of a trade secret, the two may,

85. Radin, *supra* note 41; *see also* Henderson & Yarbrough, *supra* note 41, at 19 (describing, as an example, proposed security legislation for the Health Insurance Portability and Accountability Act of 1996).

86. *See supra* notes 41–47 and accompanying text (enumerating types of unauthorized activities that raise website operators' concerns regarding damage to systems per se).

87. HOWSTUFFWORKS, *supra* note 42.

88. *See generally* ZHU ET AL., *supra* note 33, § 3 (discussing the issues arising as a result of this aggregation).

in fact, amount to the same thing.[89] Nonetheless, it is worth separating the two concepts for the purposes of this discussion on the assumption that misappropriation arguably involves more than mere access, as some of the following examples will demonstrate.

As noted above, even concerns about viruses and Web aggregators can be explained in terms of the above categories of conduct.[90] In fact, even the difficult-to-address area of DDoS attacks might be explained in terms of damage to or destruction of information, if that category were interpreted as being broad enough to encompass damage to a complainant's (or its customers') ability to access and use its own information. Perhaps this sounds far-fetched, but the generic concern about damage to or destruction of information is premised largely on the loss of the owner's ability to use the information. As with damage or destruction of a tangible, physical asset, the owner's concern is with deprivation of the asset by the wrongdoer. A DDoS attack effectively deprives the owner of the relevant assets, at least temporarily.

An owner of property rights in information obviously wants to exert a significant degree of control over the item in question[91] and to generate profits from utilizing the item in commerce. An owner's control might take the form of licensing the information, selling it, utilizing it as collateral for a loan,[92] etc. In order to preserve the ability to utilize the item in these ways, an owner's control of the item must extend to the ability to limit *access* to the item and exclude others from using it. Otherwise, there would be no potential to license or transfer it for valuable consideration as others could simply take it free of charge. The owner must also be able to guard against *unauthorized uses and/or disclosures* of the information that might impact the information's value negatively, again by increasing its general availability.

Owners of proprietary information will also want to guard against damage to or destruction of the information for the reasons set out

89. The possibility of access and misappropriation being the same is taken up in greater detail in Part IV.

90. *See supra* text accompanying and following note 86 (noting damage and distribution of information concerns).

91. *See* Lipton, *Framework*, *supra* note 14.

92. This is a more unusual use of information property, but commentators have been suggesting ways in which security may be asserted over cyber-age information assets. *See* Alice Haemmerli, *Insecurity Interests: Where Intellectual Property and Commercial Law Collide*, 96 COLUM. L. REV. 1645, 1651–52 (1996) (noting examples of major bankruptcies and creations of new deals where investments were secured by intangible, copyrighted assets); Xuan-Thao Nguyen, *Intellectual Property Financing: Security Interests in Domain Names and Web Contents*, 8 TEX. WESLEYAN L. REV. 489, 490 (2002) (arguing that, without perfected security interests under Article 9 of the Uniform Commercial Code, lenders and investors will lose security rights in online, intangible assets when bankruptcies occur).

above. Property owners require protection against those who would deprive them of their proprietary rights, whether or not the wrongdoer actually profits from the deprivation.

The same may be true of theft or misappropriation of information. Property owners will seek legal sanctions against such conduct because it potentially deprives them of their property, whether or not it benefits another. In the information property context, theft or misappropriation can work differently than it does in the physical world because of information's non-rivalrous[93] quality. Because information can exist in more than one place at the same time, a policy decision must be made as to whether theft or misappropriation in this context necessarily connotes a physical deprivation of the information, or rather a taking of the information in the sense of "copying." In other words, can there be misappropriation of information if the initial owner is not deprived of the information per se, but the value of the information is eroded because it is now available from more than one source? The latter is more likely and representative of trade secret law in relation to unauthorized misappropriations of information.[94]

Thus, concerns with the four categories of unauthorized conduct all really amount to the need to achieve at least one of two possible outcomes: (a) the preservation of the commercial value of the information in the hands of its owner, and/or (b) the preservation of the information per se in the hands of its owner.

Concerns about unauthorized access, use, and misappropriation are all premised on the first outcome—the preservation of the commercial value of the item by maintaining its scarcity in the market. The concern about unauthorized damage or destruction of the item is based more squarely on the premise of preserving the actual information per se in the hands of its owner.

Clearly, it is now possible to suggest a framework for the protection of information property rights against unauthorized bad faith intrusions organized around the four activities described above for the policy reasons also detailed above. Part IV illustrates that the current pastiche of laws in the United States and the European Union protecting information actually does contemplate prohibitions against most of these activities and for these reasons. The current laws simply are not

93. *See supra* note 62 (describing how information can be a "public good" (meaning information can be shared easily among many people at the same time)).

94. *See* UNIF. TRADE SECRETS ACT § 1(2) (amended 1985) (defining "misappropriation" of a trade secret without requiring a deprivation of the original owner's access to his own information).

organized in a cohesive way that clearly exemplifies the public policy basis for protecting information in these ways.

Part IV suggests that by focusing on these types of conduct and the underlying policies behind their prohibition, we can create a more transparent and internally cohesive set of laws relating to unauthorized dealings with information property. This may help lawmakers and policymakers respond more appropriately to issues involving such conduct. It may also assist with the important matter of international harmonization of laws relating to information property, an issue that will only increase in importance as society and commerce become more global.

IV. A PATCHWORK OF INFORMATION PROPERTY LAWS

This Part examines the current legal frameworks in the United States and the European Union regarding unauthorized access, use, damage or destruction to, and theft or misappropriation of valuable information. It demonstrates that it is indeed possible to take these four categories of unauthorized conduct as the basis of a legal and policy framework to organize and explain social and commercial attitudes to unauthorized dealings with valuable proprietary information. The examples described below come from various areas of law. To date, no coherent attempt has been made at creating a unifying framework for these areas to ensure that the relevant categories of conduct, in relation to different kinds of valuable information, are treated in a harmonized fashion.

The examples presented in this Part are not necessarily comprehensive, but they are some of the most obvious areas in which laws have been created in a piecemeal fashion to address unauthorized dealings with various types of valuable information. The three types of potentially valuable information addressed in the following discussion are (a) trade secrets and business methods, (b) valuable software (copyrighted and/or patented), and (c) unoriginal databases.[95] These examples have been chosen as some of the most obvious information products that may constitute key valuable assets of an online business.

95. "Unoriginal databases" in the sense that they are not sufficiently unique for copyright protection. *See generally* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340 (1991) (concluding that factual compilations of telephone numbers, or other unprotectable data, can only be original for copyright protection if the arrangement of the data is sufficiently unique and not an organizational method commonly employed by others working with that data).

A. The United States Position

Table 1 (below) summarizes the U.S. legal position in relation to unauthorized access, use, damage or destruction, and theft or misappropriation of these items. A similar table is provided in Part IV.B in relation to the European Union position on these activities.

Table 1: United States Law on Unauthorized Dealings with Valuable Information Products

	Unauthorized Access	**Unauthorized Use**	**Damage or Destruction**	**Theft or Misappro-priation**
Trade Secrets/ Business Methods	Unauthorized uploading and downloading of trade secrets are offenses under federal Electronic Espionage Act	Unauthorized use and disclosure prohibited under Uniform Trade Secrets Act and Electronic Espionage Act	Some prohibitions under Electronic Espionage Act	Civil and criminal liability under Uniform Trade Secrets Act and Electronic Espionage Act, respectively
Software (copyrighted)	Digital Millennium Copyright Act: civil and criminal penalties for unauthorized access	Sanctions depend on type of use; copying will not be allowed without authorization unless fair use defense applies	No obvious sanction under copyright law; may be indirect sanctions under chattel trespass law or Computer Fraud and Abuse Act	No obvious sanction unless the software is also protected by trade secrecy (see above)
Software (patented)	No legal sanction: access is permitted; patent recorded in public register	Patent Act prohibits unauthorized use subject to some defenses	No obvious patent law sanction, although may be civil and criminal liability for damage or destruction of actual data or system	No obvious patent law sanction; not possible to "steal" an invention that has already been patented; unauthorized *use* will attract patent sanction

	Unauthorized Access	**Unauthorized Use**	**Damage or Destruction**	**Theft or Misappro-priation**
Unoriginal Databases	No statutory sanction, but may be action for breach of contractual license	No statutory sanction, but may be action for breach of contractual license	No obvious direct sanction; may be indirect sanctions under chattel trespass law or Computer Fraud and Abuse Act	No obvious statutory sanction unless database contents are protected by trade secrecy (see above); may be breach of contractual license

1. Trade Secrets in the United States

Some explanation of Table 1 is necessary for those who are unfamiliar with one or more of the laws described therein. Most of the relevant legal sanctions for unauthorized dealings with trade secrets in the United States are found in the Uniform Trade Secrets Act and the Economic Espionage Act.[96] There are some significant differences between the two legislative schemes, which lead to some gaps in relation to legal sanctions for specific types of conduct.

The Uniform Trade Secrets Act is a model state law that deals with civil sanctions, such as injunctions[97] and awards of damages,[98] for misappropriations[99] of trade secrets.[100] A "misappropriation" is an unauthorized "acquisition"[101] or an unauthorized "disclosure or use"[102] of a trade secret. These prohibitions would apply to the unauthorized access,[103] unauthorized use,[104] and theft or misappropriation[105] categories of conduct suggested above as building blocks for a

96. Economic Espionage Act of 1996 § 101, 18 U.S.C. §§ 1831–1832 (2000).

97. UNIF. TRADE SECRETS ACT § 2.

98. *Id.* § 3.

99. *Id.* § 1(2) (defining "Misappropriation").

100. *Id.* § 1(4) (defining "Trade Secret").

101. *Id.* § 1(2)(i).

102. *Id.* § 1(2)(ii).

103. Here the assumption is made that unauthorized acquisition of a trade secret is tantamount to unauthorized access as outlined *supra* text accompanying note 89.

104. Unauthorized use is clearly and expressly prohibited in the definition of misappropriation. UNIF. TRADE SECRETS ACT § 1(2)(ii).

105. Theft or misappropriation is clearly contemplated in the definition of "misappropriation." *Id.* § 1(2). See in particular § 1(2)(i) on unauthorized "acquisition" of a trade secret.

framework for protecting proprietary information against unauthorized bad faith incursions. However, there is no clear sanction under the Uniform Trade Secrets Act for damaging or destroying a trade secret.

The Economic Espionage Act, on the other hand, provides legal sanctions for all four categories contemplated above: (a) unauthorized access, [106] (b) unauthorized use,[107] (c) damage or destruction of a trade secret,[108] and (d) theft or misappropriation of a trade secret.[109] The Economic Espionage Act is limited in a number of ways by constitutional limitations on federal legislative power. Notably, the offenses are limited to situations in which the wrongdoer either: (a) intends that the offense will benefit a foreign government, foreign instrumentality, or foreign agency;[110] or (b) intends to convert a trade secret related to, or included in, a product that is produced for, or placed in, interstate or foreign commerce.[111] The act is also limited to criminal sanctions. Thus, there is no power under the legislation for individual complainants to take direct civil action against a wrongdoer.

The trade secret example illustrates that the laws have indeed focused on the classes of conduct identified above as constituting a potential framework for the protection of information property rights. However, because of the federal constitutional balance and the fact that no one has necessarily considered the broader problem of protecting information property rights through the lens of a clear and cohesive policy framework more generally, some gaps have appeared in the legislation. For example, there is no direct individual civil remedy available for a complainant who has had a trade secret damaged or destroyed by a wrongdoer, although a federal criminal prosecution may be possible in some circumstances.

As noted in the Introduction, if a trade secret resides in a digital information system, currently there may be actions available under the common law of chattel trespass or under the Computer Fraud and Abuse Act ("CFA") for interference with a computer system that damages a trade secret contained therein. This Article, however, argues in favor of focusing information property laws more directly on information per se, rather than on systems within which information may be stored. If the complainant's concern is with economic loss caused by damage to or

106. Economic Espionage Act of 1996 § 101, 18 U.S.C. §§ 1831(a)(2), 1832(a)(2) (2000) (making it a criminal offense to download or upload a trade secret without authorization).

107. *Id.* (making it a criminal offense to copy, photograph, alter, transmit, etc., a trade secret).

108. *Id.* (making it an offense to destroy a trade secret without a requirement of "damage").

109. *Id.* §§ 1831(a)(1), 1832(a)(1).

110. *Id.* § 1831(a).

111. *Id.* § 1832(a).

destruction of a trade secret, then there should be a law that deals directly with that issue. This is where a clear and cohesive policy framework for protecting information property rights may be useful.

2. Software in the United States

The second and third rows of Table 1 deal with unauthorized interferences with various intellectual property rights in computer software. The Table does not take into account the fact that valuable proprietary software can also acquire protection from contractual and technological protection measures, although these are clear possibilities.[112]

In terms of intellectual property protection, both copyright and patent laws deal predominantly with unauthorized uses of the property in question. Copyright law is concerned largely with unauthorized reproduction of the work,[113] and patent law is concerned with unauthorized use and commercial exploitation of the invention.[114] Neither copyright law nor patent law traditionally has been concerned with unauthorized *access* to a work per se. However, in recent years the Digital Millennium Copyright Act[115] ("DMCA") has legally bolstered the effect of technological protection measures that seek to restrict or prevent access to a copyright work.[116]

Copyright and patent laws also have not focused specifically on unauthorized damage or destruction, or theft or misappropriation. Again, if the copyrighted or patented software resides in a digital information system and a wrongdoer gains unauthorized access to the system for the purposes of, or with the effect of, damaging or misappropriating the software, remedies may be available to the complainant under the law of computer trespass[117] and/or under the

112. Fisher, *supra* note 72, at 1203 (predicting that producers of intellectual property products suitable for distribution on the Internet will increasingly rely on contractual and technological protection measures rather than simple intellectual property rights to protect their interests in relevant digital products); *id.* at 1211 (setting forth the possibility of using contract and technology to create a more generous set of property rights for a digital product holder than intellectual property law alone would provide).

113. BRUCE A. LEHMAN, INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS 63–64 (1995).

114. *Id.* at 155.

115. Digital Millennium Copyright Act § 103, 17 U.S.C. §§ 1201–1205 (2000).

116. The DMCA basically prevents the circumvention of technological protection measures that restrict access to a copyrighted work and the trafficking in devices that facilitate such circumvention. *Id.* § 1201.

117. *See* CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp 1015, 1021–23 (S.D. Ohio 1997).

CFA. Again, however, these laws often tend to focus on unauthorized access to a *system* rather than dealing more directly with concerns about damage to software stored within a system.

Again, this might be an area where focusing policy debates squarely on the need to restrict unauthorized conduct in relation to proprietary information would provide a clearer framework. Currently, the DMCA deals with *access* rather than *use*. This is a very uncharacteristic focus for copyright law, which traditionally deals with prohibited and permitted *uses* of a work, rather than with the ability to *access* a work. A more cohesive framework may help to streamline approaches to unauthorized access to, and use of, information.

3. Databases

The fourth row of Table 1 deals with the increasingly vexing question of property rights in databases that are not necessarily sufficiently original in the selection or arrangement of their contents to attract copyright protection.[118] This may be the majority of valuable digital databases, as their value tends to lie in their comprehensiveness and unselectiveness.[119] Likewise, their arrangement tends not to be particularly original as the contents are usually input and stored in standard formats and accessed through the use of search engines.

A number of bills have been drafted in an attempt to create sui generis proprietary protection for databases in the United States,[120] but Congress has not yet enacted anything satisfactory. A significant impetus for drafting these bills was that the European Union created such legislation under the auspices of the E.U. Database Directive,[121] and there was initial concern that if the United States did not follow suit, American businesses might be disadvantaged vis-à-vis their European Union counterparts.[122]

There are a number of reasons why legislation in the United States has not yet materialized in final form. The reason for the delay relates in part to timing and legislative priorities. Yet, there have also been

---

118. *See* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340 (1991); *see also supra* note 95 and accompanying text (defining unoriginal databases).

119. Brown et al., *supra* note 51, para. 61 (discussing when electronic databases qualify for copyrights).

120. *E.g.*, Collections of Information Antipiracy Act, H.R. 354, 106th Cong. (1999); Consumer and Investor Access to Information Act of 1999, H.R. 1858, 106th Cong. (1999); *see also* Lipton, *Balancing Private Rights*, *supra* note 13, at 803–05 (describing U.S. congressional attempts at creating database protection).

121. E.U. Database Directive, *supra* note 36.

122. Julie Wald, *Legislating the Golden Rule: Achieving Comparable Protection Under the European Database Directive*, 25 FORDHAM INT'L L.J. 987, 1027 (2002).

significant concerns expressed about drafting a law that strikes an appropriate balance between protecting proprietary rights in databases and preserving sufficient good faith access to database contents.[123]

As noted in the Introduction, it is important for Congress to clearly identify and protect appropriate good faith uses of relevant information and bolster legal protections against bad faith conduct when granting information property rights. Although this Article is focused on restricting such bad faith conduct, it is important to appreciate that the arguments presented here do not advocate a general over-commodification of information products. Any laws that protect information property rights should do so in a balanced manner and should limit and restrict bad faith activities that would damage information property holders' interests; they should also do so while preserving socially appropriate good faith uses of information, such as fair use in copyright law.[124]

Given that there is no specific statutory property right in databases in the United States, other than the protection for original selection and formatting provided under copyright law,[125] there are clearly no direct legal sanctions for unauthorized access, unauthorized use, damage, or misappropriation of database contents per se. Private sanctions may be imposed by contract law, and indirect sanctions may arise in terms of laws that restrict or prohibit unauthorized interference with a computer system.[126] Nonetheless, for the reasons detailed above,[127] this approach is not completely satisfactory. There are no clear and cohesive sanctions for unauthorized dealings involving proprietary databases. If a sui generis database law does arise in the United States, it will deal

123. Good faith uses might include uses of data for scientific, technological, and educational purposes. *See* Reichman & Uhlir, *supra* note 18, at 831–32 (postulating the need to preserve educational and scientific uses of information in the wake of the creation of private property rights in databases). Teaching and educational purposes may also be relevant here. *See* Copyright and Rights in Databases Regulations, (1997) SI 1997/3032 § 20(1)(b) (Eng.) (allowing an exception for the use of database contents only for educational and research purposes).

124. Fair use is a limitation on the exclusive rights of a copyright holder. The doctrine is intended to balance the copyright holder's proprietary rights in a work against allowing certain uses, such as criticism, commentary, news reporting, teaching, scholarship, or research. Whether a particular use is a fair use requires balancing at least four factors: (1) commercial uses versus non-profit educational uses; (2) the nature of the copyrighted work, such as whether it is unpublished, factual, or fictitious; (3) the quantity of the work being copied; and most importantly, (4) the economic effect of the use. 17 U.S.C. § 107 (2000); *see also* LEHMAN, *supra* note 113, at 73–80.

125. Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., Inc., 499 U.S. 340, 348 (1991).

126. For example, chattel trespass laws and relevant provisions of the CFA.

127. *See supra* notes 30–34 and accompanying text (explaining the shortcomings of the chattel trespass approach).

with some aspects of such unauthorized dealings. A glimpse at the European Union law (below) might suggest how this could be done, although the European Union approach has not gone without its critics.[128]

Importantly, the development of a law and policy framework that organizes our thinking about how the law should respond generally to unauthorized incursions into information property rights could be an important step in creating an appropriate sui generis database law for the United States. Such a framework could help to identify and isolate the types of bad faith conduct about which database producers might reasonably be concerned. It also might organize appropriate legal responses to those concerns in the context of larger concerns about protecting the integrity of information property rights more generally.

B. The European Union Position

As in the United States, legislatures throughout the European Union have grappled with problems relating to the protection of various classes of information property rights against unauthorized access, use, damage or destruction, and theft or misappropriation. Some of the relevant laws are summarized in Table 2.

Table 2: European Union Law on Unauthorized Dealings with Valuable Information Products

	Unauthorized Access	**Unauthorized Use**	**Damage or Destruction**	**Theft or Misappropriation**
Trade Secrets/ Business Methods	Law varies among Member States; English law based on "relationships of confidence" in contract and equity	Law varies among Member States; English law based on "relationships of confidence" in contract and equity	Law varies among Member States; where the information is not property, as in England, there may be no obvious remedy	Law varies among Member States; English law based on "relationships of confidence" in contract and equity

128. Catherine Colston, Sui Generis *Database Right: Ripe for Review?*, 2001(3) J. INFO. L. & TECH., *at* http://elj.warwick.ac.uk/jilt/01-3/colston.html; Reichman & Samuelson, *supra* note 10, at 77–80, 83–84.

	Unauthorized Access	Unauthorized Use	Damage or Destruction	Theft or Misappropriation
Software (copyrighted)	E.U. Copyright Directive, Art. 6 prevents circumventing a technological protection measure to access a copyright work[129]	Copyright legislation in most Member States will prohibit reproduction or copying without authorization, unless a defense like fair use applies	No obvious direct sanction other than perhaps tort law sanctions for chattel trespass	No obvious direct sanction other than perhaps tort law sanctions for conversion or misappropriation.
Software (patented)	No legal sanction. Access is permitted; patent recorded in public registers	Member States' patent laws will prohibit unauthorized uses	No obvious patent law sanction, although may be civil and criminal liability for damage or destruction of actual data or system	No obvious patent law sanction; not possible to "steal" an invention that already has been patented; unauthorized *use* will attract patent sanction
Unoriginal Databases	No obvious legal remedy, although may be contractual restrictions on access to a particular database	Unauthorized "extraction" and "reutilization" of substantial part of database contents are prohibited under the Database Directive	No sanction under Database Directive, but since the database right is a personal property right, there might be a tort action in chattel trespass	Unauthorized "extraction" and "reutilization" of substantial part of database contents are prohibited under the Database Directive

129. Council Directive 2001/29/EC of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in Information Society, 2001 O.J. (L 167) [hereinafter E.U. Copyright Directive], *available at* http://europa.eu.int. This provision is much like the DMCA in the United States. It has proved controversial in some European Union Member States and has not been implemented yet into domestic law in the United Kingdom (as of May 5, 2003), despite the passing of the deadline for implementation in December 2002.

There are many obvious similarities between Table 2 and Table 1. The points of distinction between the two relate mainly to trade secrets and unoriginal databases. These differences do not necessarily evidence a divergence of underlying approaches to the protection of commercially valuable information generally, as the following discussion demonstrates.

It is important to recognize that Table 2 differs from Table 1 in that many of the relevant issues in the European Union are covered under individual laws of Member States and not under legislation enacted in compliance with a European Union directive.[130] This does not necessarily mean that these laws are not well harmonized. In fact, intellectual property laws are generally relatively well harmonized throughout the European Union, at least in theory.[131] Table 2, therefore, refers to things like "Member States' patent laws." This is unavoidable, as it is beyond the scope of this Article to investigate all the individual Member States' specific laws relating to information property rights.

In fact, the comparison illustrates what has largely been the major problem with legislating to protect the integrity of commercially valuable information property rights in both the United States and the European Union to date. Previous approaches have taken a case-by-case approach to legislation, focusing on a specific class of information asset. Thus, there are laws relating to trade secrets and laws relating to unoriginal databases. There has been no overall framework for laws that protect the integrity of valuable commercial information generally. Such an approach arguably might help to better organize and, ultimately, harmonize laws relating to information property rights by clarifying their underlying policy objectives.

1. Trade Secrets in the European Union

It is not surprising that the United States and the European Union laws diverge on trade secrets and databases. In the case of trade secrets, the United States arguably has much more well developed laws than

130. A European Union Directive must be implemented into domestic law by all European Union Member States, usually within two years of the finalizing of the Directive. The point is to ensure that Member States' laws harmonize on the points covered in the Directive. For more detail on the legislative and other processes of the European Union, refer to http://europa.eu.int.

131. Much of the European Union law on traditional intellectual property rights and some new sui generis rights are based on a combination of World Intellectual Property Organization ("WIPO") treaties and European Union Directives. Although there are differences of interpretation amongst European Union Member States, the basic principles of intellectual property law are relatively well harmonized.

most other jurisdictions. The United States is one of the only jurisdictions in the world, if not the only one, that has enacted specific trade secret legislation, as opposed to leaving the issue of trade secret protection to the common law.[132] This position is reflected in the first row of Table 2, which takes, by way of example, the English 'trade secret' law, largely based on contract and equity principles. English courts can impose sanctions for misuse or misappropriation of a commercial confidence.[133] However, the sanction emerges from a contractual[134] and/or equitable relationship between the parties[135] and not from a proprietary interest in the information in question.[136]

The United States, on the other hand, has recognized clear proprietary rights in valuable trade secrets.[137] The judiciary[138] and both state and federal legislatures[139] have recognized these property rights. Yet, this fact alone does not mean that the U.S. and English legal systems are not doing very similar things in practice when they protect trade secrets. Professor Raymond Nimmer has provided a useful analysis of the U.S. approach to trade secret protection that may assist with this comparison:

> Describing a [trade] secret as a form of property is particularly useful in analyzing the circumstances under which trade secrets can be conveyed through a license, assignment, or sale.... However, describing a trade secret as property can create misleading inferences. The idea of property is itself ambiguous. Describing something as a property right often means that the owner has a legal right to exclude all others from using or exercising control over the property. For traditional types of property, this view has numerous exceptions; for trade secrets, the exceptions also define the general rule.
>
> ....
>
> In trade secrecy, the right to exclude others depends on the secrecy maintained by the owner of the secret and by the confidentiality he or

132. This is the position taken in jurisdictions such as the United Kingdom and Australia. *See* W.R. CORNISH, INTELLECTUAL PROPERTY: PATENTS, COPYRIGHT, TRADE MARKS AND ALLIED RIGHTS, ¶¶ 8-06 to 8-09 (4th ed. 1999) (describing the equitable and contractual basis for the breach of confidence action in the United Kingdom); JILL MCKEOUGH & ANDREW STEWART, INTELLECTUAL PROPERTY IN AUSTRALIA, ¶¶ 3.4–3.8 (2d ed. 1997) (describing equitable and contractual basis for the breach of confidence action in Australia).

133. CORNISH, *supra* note 132, ¶ 8-10 (noting that sanctions are also available for misuse or misappropriation of technical, personal, and other information).

134. *Id.* ¶ 8-06.

135. *Id.*

136. *Id.* ¶¶ 8-49 to 8-53.

137. Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1003–04 (1984).

138. *Id.*

139. Economic Espionage Act of 1996 § 101, 18 U.S.C. §§ 1831–1839 (2000), *amended by* Criminal Law Technical Amendments Act of 2002, Pub. L. No. 107-273, § 4002(e)(9), 116 Stat. 1806, 1810.

> she imposes on those to whom the secret is revealed. Trade secret law conveys no exclusive rights independent of these factors. Therefore, it does not preclude independent discovery and subsequent use. The proprietary rights in a trade secret are linked to the legal concepts of misappropriation and breach of confidential relationships. The property interest arises through and is defined by the legal system's willingness to enforce such relationships.
>
> Thus, when a trade secret is described as property, that is not to say that there is a property interest in the information such as could be enforced against the world at large. Rather, the value lies in the information *and* the network of secrecy and confidentiality agreements created around it by its "owner." U.S. law is willing to protect that value.[140]

I have included this quote at length because it illustrates two important points about trade secret protection that are relevant to this discussion. The first is that Professor Nimmer illustrates the importance of the property metaphor when dealing with an item with which one wants to deal in commerce. He suggests that the importance of accepting as property something that might not otherwise fall within more traditional definitions of property lies in the usefulness of that characterization for thinking about commercial transactions involving licensing, sale, other forms of assignment, etc.

Professor Nimmer's suggestion supports the arguments presented in Part II.C about the importance of lawmakers and policymakers accepting property rights in valuable information because that is what the market will demand regardless of the level of support it receives from the law.[141] It makes sense for the law to reflect societal attitudes in this respect, provided that law and policy makers are alert to prevent the over-propertization of information, beyond what might reasonably be expected in society and commerce.

Professor Nimmer's comments also emphasize the underlying similarities between the American and English approaches to trade secret protection. Despite the fact that English legislatures and courts have not accepted a property label for valuable trade secrets, they have protected the integrity of those secrets in much the same way as legislatures and courts have in the United States. Under both systems, protection is really being extended to the owner's efforts to keep the information secret by imposing obligations of confidence on those to

---

140. 1 RAYMOND T. NIMMER, THE LAW OF COMPUTER TECHNOLOGY: RIGHTS, LICENSES, LIABILITIES § 3.3 (3d ed. 1997) (footnote omitted).

141. *See supra* Part II.C (explaining the motivations for creating property rights—specifically that legislators tend to follow market needs in establishing property rights).

whom the information might be disclosed, and perhaps also by taking other measures, such as utilizing encryption devices.

Thus, despite Professor Nimmer's suggestion that trade secrets are not really property in the sense that they are not theoretically enforceable against the world at large, it may be that as laws and technologies have developed to meet market expectations, such secrets are now enforceable in this way. An example would be a company that stores its valuable information electronically, preventing access to the information by the use of strong encryption measures and imposing strict contractual obligations of confidence on anyone to whom the information is disclosed. Thus, despite the technical differences in legal approach between the United States and some other jurisdictions regarding the protection of valuable trade secrets against unauthorized accesses and uses, the underlying policy concerns are very similar.

2. Databases in the European Union

As noted above, the second major point of distinction between Table 1 and Table 2 relates to protecting unoriginal databases against unauthorized interference. Here, the difference between the United States and the European Union is more striking than in the case of trade secrets. U.S. law provides no distinct proprietary protection for databases that are insufficiently original in the selection or arrangement of their contents to attract copyright protection.[142] Even those databases that do attract copyright protection will only attract copyright in the literal expression of that original selection or arrangement, not in the contents per se.[143] The same result on copyrightable databases follows in the European Union. European Union Member States have preserved copyright protection in literal expressions of databases where the selection or arrangement of their contents is original for copyright purposes.[144]

On the other hand, database producers have expressed concerns about proprietary protections for their database contents as opposed to the literal expression of those contents.[145] In the European Union, these

142. Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 362–64 (1991).

143. As noted above, copyright will only protect the literal expression of a compilation and not its contents. *See supra* notes 74–75 and accompanying text.

144. E.U. Database Directive, *supra* note 36, art. 3(1).

145. JUSTIN HUGHES, POLITICAL ECONOMIES OF HARMONIZATION: DATABASE PROTECTION AND INFORMATION PATENTS 10–51 (Cardozo Law School, Public Law Research Paper No. 47, July 8, 2002) (discussing the political and market forces behind the debates on database protection legislation in the United States and in other jurisdictions), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=318486 (last visited Oct. 12, 2003).

concerns led to the drafting of the E.U. Database Directive.[146] This created a new class of sui generis property rights in databases based on the substantial efforts of their compilers.[147] As Table 2 demonstrates, this new property right prohibits the unauthorized extraction and/or re-utilization of a substantial part of a protected database's contents.[148]

These prohibitions probably map onto the unauthorized use and misappropriation categories of conduct described above. An "extraction" is arguably a misappropriation, and a "re-utilization" would clearly be a use. Thus, there is no direct prohibition under the E.U. Database Directive for unauthorized access or for damage or destruction to the contents of a protected database.

Access may be prohibited through the use of restrictive contractual provisions and encryption measures as in the United States. Damage or destruction may also be captured as a result of the individual Member State laws that prohibit unauthorized access to a computer system,[149] much along the lines of the U.S. computer trespass action or the prohibitions on unauthorized access under the CFA.[150] In fact, access to the *data* per se also may be prohibited indirectly under provisions barring access to the *system* in which the data is stored. However, as noted above, if what we are really concerned about in the modern digital age is damage to data per se, our laws should reflect this concern more clearly and directly.

There is a clear expectation by those who compile valuable databases that they "own" proprietary or quasi-proprietary rights in those databases. Whether there are clear statutory property rights, as in the European Union,[151] or market-driven contractual rights, as in both the United States and the European Union, database producers are clearly asserting some form of proprietary right in a valuable information product.

The question for lawmakers and policymakers is how best to protect database producers from bad faith incursions, while preserving good faith access to database contents. The second part of this equation—the protection of good faith access such as fair use type activities in

146. *Id.* at 18–27 (discussing E.U. Database Directive).

147. E.U. Database Directive, *supra* note 36, art. 7(1).

148. *Id.*

149. Interestingly, the Computer Misuse Act, 1990, c. 18, § 3 (Eng.), does not contemplate damage or destruction of data as an offense punishable under the statute. However, preventing or hindering access to data is an offense. *Id.* § 3(2)(b).

150. *See, e.g.*, 18 U.S.C. §1030(a)(5)(A) (2000) (contemplating penalties for the damage or destruction of data stored within a federal computer system).

151. E.U. Database Directive, *supra* note 36, art. 7(1).

copyright law—is beyond the scope of this Article, although scholars have discussed it in detail elsewhere.[152]

Assuming that this part of the equation can be addressed adequately by legislators,[153] the other part of the equation relates to streamlining and harmonizing the approach to organizing those aspects of the law that will actually prohibit unauthorized bad faith incursions into the information property contained in valuable databases. In this Article, I suggest that legislators should consider this question in the context of a broader "information property" policy framework that focuses on protecting all forms of valuable information property against bad faith access, use, damage or destruction, and misappropriation.

Obviously, dealing with the over-propertization concerns regarding databases is a tall order. This tall order is one reason why the E.U. Database Directive has attracted so much criticism[154] and why the United States Congress has not settled on a legislative approach.[155] Additionally, the approach taken to the over-propertization question is likely to affect the form of laws that prevent bad faith access and use of valuable databases. Professors Reichman and Samuelson, for instance, advocate a tort/misappropriation approach to database protection.[156] This approach implicitly involves the classification of certain accesses and uses of database contents as being in good faith or bad faith. It prohibits misappropriations that create unfair commercial advantages.[157] Effectively, this is how "bad faith" is conceptualized under this suggested model. This approach is also evident to some extent in at least one of the bills drafted in the United States to protect database producers.[158]

If the question of protecting legitimately asserted property interests in information products can be addressed under a broader cohesive

152. Lipton, *Balancing Private Rights*, *supra* note 13, at 798; Reichman & Samuelson, *supra* note 10, at 70–73; Reichman & Uhlir, *supra* note 18, at 811–12.

153. This is a difficult question and has, to date, been a key reason why acceptable database protection legislation has not been enacted yet in the United States. *See* HUGHES, *supra* note 145, at 29 (noting that opposition from American research and library communities complicated the issue of database protection legislation during the WIPO process of drafting an international database protection treaty).

154. Reichman & Samuelson, *supra* note 10, at 84–95 (criticizing the scope of the E.U Database Directive and discussing the resulting weaknesses); *see also* Colston, *supra* note 128, § 2.3 (discussing the broad definition of the sui generis right).

155. HUGHES, *supra* note 145, at 10–11.

156. Reichman & Samuelson, *supra* note 10, at 140–44.

157. *Id.* at 141–43.

158. Consumer and Investor Access to Information Act of 1999, H.R. 1858, 106th Cong. § 102 (1999). The aim of this bill is to prevent unfair commercial conduct by distribution of wholesale copies of a database in direct competition with the original database producer.

framework such as that suggested in this Article, it may usefully inform the development of database protection law per se. Legislators would be able to focus on all potential aspects of bad faith conduct in relation to a database, such as access, use, damage or destruction, and theft or misappropriation at the same time. This might enable legislators to more effectively counterbalance acceptable good faith uses of information against unacceptable bad faith incursions in a more harmonized and consistent manner.

V. CONCLUSION: FUTURE APPROACHES TO INFORMATION PROPERTY

The above comparisons of the patchwork of laws within the United States and the European Union dealing with bad faith intrusions into proprietary information products evidence that the underlying concerns between jurisdictions and among different classes of information assets are largely the same. Those holding valuable information assets are seeking first to assert a form of a property or quasi-property right in their assets to facilitate commercial dealings in the assets and, second, to protect those assets against bad faith access, use, damage or destruction, and theft or misappropriation.

This Article suggests that there might now be an opportunity to reformulate laws relating to the protection of information property against bad faith interferences by utilizing a more unified and cohesive policy framework than was used in the past. Of course, difficult issues have arisen in both the United States and the European Union regarding the assertion of legal property rights in many information assets. This Article does not seek to belittle the difficulties arising in this area. Any laws that create and/or promote the assertion of property rights in information should be drafted realistically in a manner that is sensitive to competing good faith interests in information.[159]

As noted in Part II.C, however, regardless of what legislators do or fail to do in creating information property rights, the market itself will develop new ways to treat commercially valuable items as property to facilitate trade in those items. In the absence of trade secret legislation, individual parties have relied on contractual provisions to protect commercial confidences in the United Kingdom.[160] By the same token,

159. Competing good faith interests in information may comprise rights to privacy in relation to personal information or rights to access and use information for public interest purposes, such as scientific, educational, research purposes, etc. Lipton, *Rights and Responsibilities*, *supra* note 14.

160. In jurisdictions with a significant equitable jurisprudence, equity has also had a role to play in protecting commercial confidences. *See* CORNISH, *supra* note 132, ¶ 8-06; MCKEOUGH &

in the absence of sui generis database protection legislation, American businesses have relied on contractual provisions and technological protection measures to assert quasi-property rights in databases.

Whether or not legislators create property rights, market players will seek to limit others from accessing, using, damaging or destroying, and/or misappropriating valuable information without authorization. What legislators can do is recognize these classes of conduct as the activities that concern information property owners. Legislators can ensure that they enact a sensible and coherent framework of laws for the digital information age that protects information property owners against bad faith unauthorized conduct of these types, while permitting good faith conduct.[161]

Any such laws should focus on protecting legitimate property interests in information per se, rather than indirectly protecting valuable information through the protection of the physical, tangible attributes of information systems, such as the computers in which information is stored physically and the cables through which it may be disseminated physically. In the words of Dane McLeod, the laws should focus on the data rather than the box to achieve the desired policy results.[162]

These results could be achieved in a variety of ways. One very simple approach would be to retain the category-specific laws that are currently organized around different types of information, but to develop those laws in accordance with the express policy of protecting each class of information property against unauthorized access, use, damage or destruction, and theft or misappropriation.

Thus, there still would be completely separate types of property interests in different information assets, such as software and databases. Software might attract copyright and/or patent protection as it currently does. Databases might be protected under copyright law in some jurisdictions and/or through a sui generis scheme in others. However, as each of those fields of law develops in relation to those specific information assets, legislators would keep in mind the basic framework of preventing unauthorized access, unauthorized use, damage, and/or misappropriation of these items by those with bad faith motives.

STEWART, *supra* note 132, ¶ 4.14 (noting the important role of equitable jurisprudence relating to third party liability).

161. As noted above, good faith interests in information may comprise rights to privacy relating to personal information or rights to access and use information for public interest purposes, such as scientific, educational, and research purposes. *See supra* note 159 and accompanying text.

162. McLeod, *supra* note 1, at 350–52.

Another approach might be to develop an entirely new field of information property law that would group together all valuable information products under the generic heading of "information property," regardless of whether some of those information assets might attract the existing protections set out in Tables 1 and 2.[163] Thus, computer software, trade secrets, databases, etc. would all generically be classified as "valuable information products," and a completely new set of information property laws could be developed prohibiting bad faith conduct in terms of unauthorized access, use, damage or destruction, and/or misappropriation. This would be an ambitious project; delineating the boundaries of information property rights in the first place to avoid over-propertization concerns would present a significant challenge.

The advantage of this approach is that it would take a comprehensive and cohesive attitude toward matters of general concern to market players in the digital economy. Further, there would be little need to amend any existing laws, as the new legal framework would be unlikely to contradict provisions of current copyright, patent, trade secret, and database laws. The framework would simply fill in some of the gaps in those preexisting laws relating to the protection of information products. This approach also would remove the focus of information property law from the boxes in which information is stored and emphasize the information itself.

Focusing on the data rather than the box is a more logical approach given that market players generally are likely to be much more concerned with loss or damage to the value of their information than to physical attributes of the systems in which information is stored and through which it is transmitted. Where there is a concern with damage to a physical system due to real-world vandalism, current criminal and tort laws should deal with those situations. This is not problematic. What has been problematic in the past is the confusing emphasis on *systems* when the plaintiff's complaint is actually more likely to be about damage to the value of *information stored in the system.*

Overall, we should not worry about accepting property metaphors in cyberspace and protecting information property rights as such. We simply have to ensure that we are utilizing appropriate metaphors in appropriate ways. An information system is comprised of individual components of *tangible personal property.* The information within the system may be considered a species of *intangible personal property.*

163. Lipton, *Framework*, *supra* note 14 (suggesting the development of an information law and policy framework more generally).

None of these items should be regarded as a species of real property. The property terminology is unobjectionable if conscious attempts are made to ensure that it is not loaded with inappropriate connotations and that property rights are not allowed to lead inevitably to unfair monopolies.[164] The legal system has coped with various classes of property rights over many, many years. The property concept can be flexible enough to cope with new situations and challenges, and, importantly, it does not necessarily have to connote any particular set of rights other than those of an item of value with which people desire to trade in a market.[165]

164. Chander, *supra* note 10, at 778 (contending that property rights are never absolute and are always controllable to some degree by government).

165. *See* Litman, *supra* note 54, at 1293–96 (discussing the use of property rights regimes when alienability is of primary importance); Rao, *supra* note 54, at 364 (citing transferability of rights as the key characteristic of property).