Cybersquatting: Blackmail on the Information Superhighway

John D. Mercer[†]

I. INTRODUCTION

The present-day Internet, often called the "information superhighway," is not what its original creators imagined.[1] The Internet began in the 1960s as a Department of Defense project named ARPANET.[2] ARPANET was a computer network that allowed various countries to stay in communication during and after a catastrophe.[3] After the Cold War ended, ARPANET became the Internet, as many non-military users used the network.[4] Even after the Internet became more civilian-friendly, it was not until recently that the Internet became a commercial tool.[5] With the creation of the World Wide Web and a graphical, point-and-click interface that combines text with pictures, sounds, and easy linking, commercial users could finally take full advantage of the Internet.[6]

To establish themselves on the Internet, corporations must register a domain name.[7] Until recently, Network Solutions, Inc. ("NSI") distributed all domain names to registrants.[8] NSI did so purely on a "first-come, first-serve" basis without regard for trademark, trade name, or any other proprietary claims to the registered name.[9] Because NSI only checked for uniqueness, i.e., that no one else had already claimed the desired domain name, individuals were able to register domain names corresponding to famous trademarks with an eye towards reselling these domain names to the owners of the famous trademarks.[10] These individuals have been called "cybersquatters."[11]

Now, multiple registrars (including NSI) distribute Internet domain names. Assuming that a corporation wants to register a domain name using ".com" or ".net" as a top-level domain ("TLD"), a corporation must use a registrar accredited by the Internet Corporation for Assigned Names and Numbers ("ICANN").[12] Although ICANN-accredited registrars will still grant domain names on a "first-come, first-serve" basis,[13] these registrars now follow a uniform dispute resolution policy to decide competing claims for domain names.[14] Although this dispute resolution policy may prevent some cybersquatting, the policy's only remedy is

cancellation or transfer of the domain name registration.[15] This consequence may be inadequate to deter cybersquatting. In addition, clever cybersquatters may still be able to circumvent ICANN's dispute resolution policy.[16]

II. THE PROBLEM OF CYBERSQUATTING

A. What is Cybersquatting?

Cybersquatting is a phenomenon only as old as the World Wide Web itself.[17] Cybersquatters have been characterized as "individuals [who] attempt to profit from the Internet by reserving and later reselling or licensing domain names back to the companies that spent millions of dollars developing the goodwill of the trademark."[18] Basically, cybersquatting occurs when an individual or a corporation registers a domain name that is spelled the same as a pre-existing trademark, and demands money from the trademark owner before the registrant will release the domain name.

Individuals who register domain names corresponding with trademarks differ in character. For example, of the four major players in disputes on the Internet, two are "guilty" of cybersquatting and two are "innocent."[19] The guilty players are ransom grabbers and competitor grabbers.[20] Ransom grabbers are the paradigmatic cybersquatters; they strategically register trademarks as domain names in order to sell it to the legitimate trademark holders. Competitor grabbers are individuals or corporations that register a domain name corresponding to a competitor's trademark in order to sell their own goods on it or merely to hinder the legitimate trademark holder's use of the domain name.[21] On the other hand, innocent registrants and concurrent users of domain names are not guilty of cybersquatting. Innocent users register the domain name based on some unrelated interest in the word itself, without intending harm to a trademark owner.[22] Concurrent users are those who concurrently share the same trademark for different types of products and services and in different markets.[23] Although this article deals primarily with ransom grabbers, any complete solution must address the rights and responsibilities of all four players.

B. Why is Cybersquatting Wrong?

Although some commentators and courts have implied that cybersquatters restrict corporations' use of the Internet,[24] this does not accurately describe the harm caused by cybersquatters. Corporations are free to register many different domain names. The only real restriction on the Internet is that two owners cannot have two domain names spelled the same way.[25] Thus, in *Panavision International, L.P. v. Toeppen*, Panavision could not register "www.panavision.com" because Toeppen had already registered it.[26] If Panavision wanted "www.panavision.com" specifically, the corporation either had to pay the $13,000 that Toeppen demanded, or bring suit to have a court grant the corporation the domain name.[27] Still, had Panavision been less selective, the company could have registered any unused domain name, e.g., "www.panavision.video.com", and advertised its goods and services to consumers using that domain name.[28] Thus, cybersquatters do not prevent corporations from advertising or

establishing themselves on the Internet.

However, cybersquatters do harm corporations. By registering the most obvious name as a domain name (e.g., the name of the corporation itself), cybersquatters force corporations to find other ways to attract consumers to their Internet pages.[29] Instead of simply typing an obvious domain name for a corporation, customers are forced to use a search engine, which may cause additional confusion or delay when accessing the desired site.[30] In addition, because of the way search engines work, competitors' Internet sites could be brought up by a search.[31]

Because consumers seeking the page of a specific trademark owner will likely turn to a search engine, if initial attempts fail (i.e., if "www.trademark.com" does not give the desired page because a cybersquatter has registered the name), the trademark owner is injured in three ways. First, using a search engine will inconvenience the consumer, because he may possibly have to wade through thousands of other sites to get to the desired site.[32] Thus, this increases the customers search costs and makes it more likely that the customer will become frustrated with the trademark owner, regardless of the quality of her products or services. Second, the search engine route likely will bring up many Internet sites of the trademark owner's competitors.[33] Third, the frustration that customers face with this problem may convince customers to use alternative, non-Internet means to get the desired products. This fact, combined with the likely frustration from the search engine process might make customers, originally searching to purchase the trademark owner's products, shift their purchases to the trademark owner's competitors. Thus, cybersquatting can cause multiple injuries to a trademark owner.

C. Dilution is not the Solution

Although commentators have suggested various solutions to cybersquatting,[34] most have focused on applying trademark dilution principles to cybersquatting.[35] The notion that trademarks deserve protection from dilution began with Frank Schechter's seminal article, *The Rational Basis of Trademark Protection*.[36] This article states that trademarks should be protected from non-competing uses because it is the trademark's uniqueness that sells products.[37] Therefore, a trademark holder has a quasi-property right distinct from the goods on which it is placed.[38] It is this inherent quasi-property right that allows protection in the absence of consumer confusion.[39]

By the time the Federal Trademark Dilution Act of 1995 ("FTDA")[40] was passed, many states had already enacted legislation protecting trademarks from dilution.[41] The scope of FTDA protection encompasses only "famous" trademarks.[42] Although the FTDA offers factors that courts should consider to determine if a mark is famous,[43] the FTDA never defines the term "famous."[44] This has created much confusion, since courts have independently established their own tests for deciding whether a mark is "famous."[45]

When courts were first asked to decide the legitimacy of cybersquatting, plaintiffs brought claims alleging FTDA violations.[46] Although the FTDA claims were buttressed with other claims, e.g., ordinary trademark infringement and unfair competition, some courts decided

that since the FTDA could solve the problem it was unnecessary to address the other claims.[47] Unfortunately, by trying to quickly address the cybersquatting problem, these courts have stretched the applicability of the FTDA beyond its intended borders.

Courts have created precedents that are inclined to unfairly favor plaintiffs and cause more harm than good. First, the FTDA was only intended to protect "famous" marks.[48] Although few could argue that Panavision is not a "famous" mark, [49] one could effectively argue that trademarks like Intermatic[50] or TELETECH[51] are not the "famous" marks that Congress intended the FTDA to protect.[52] Yet, both of these latter corporations received protection from either a cybersquatter (Intermatic) or a competitor (TeleTech) for their trademarks under the FTDA.[53] If these corporations can receive protection under the FTDA, what corporations do not have "famous" marks amenable to FTDA protection?

Second, courts have expanded the FTDA in order to punish cybersquatters and others. The FTDA defines dilution as "the lessening of the capacity of a famous mark to identify and distinguish goods or services[.]"[54] Thus, under the FTDA, only "blurring," and not tarnishment, is captured by the statutory term "dilution."[55] Courts have expanded the definition of "blurring" to include actions that reduce the ability of trademark owners to "identify and distinguish its goods and services by means of the Internet."[56] The FTDA, even when applied as intended by Congress, already gives trademark owners too much protection.[57] Thus, this broadening of actionable "blurring" will likely cause even more problems.

Third, courts have unnecessarily expanded the meaning of "commercial use" in order to capture cybersquatting behavior. For example, in *Intermatic v. Toeppen*, Toeppen placed pictures of his hometown, Champaign-Urbana, Illinois, on the domain site "www.intermatic.com." [58] Although the court did not go so far as to say that merely owning a web site is a "commercial use,"[59] the court found that the cybersquatter's "intention to arbitrage the 'intermatic.com' domain name was a commercial use."[60]

Noncommercial uses of "famous" marks are not precluded by the FTDA, which specifically exempts such use from liability.[61] Moreover, Professor McCarthy's treatise on trademark law states that:

> dilution by blurring is triggered by presenting customers with two commercial sources under the same mark, not by foreclosing the senior user from a particular venue or medium for advertising its mark. A non-trademark use of a famous mark does not dilute. Undoubtedly, the [*Panavision*] court stretched the law to reach the reprehensible actions of a cybersquatter.[62]

By expanding the definition of "commercial use," courts have created a bad precedent that may severely hinder true "noncommercial" users of web sites.[63]

Based on precedent, there is nothing limiting courts from applying "commercial use" analysis against innocent registrants who have legitimately registered domain names that incidentally correspond to trademarks. For example, a hypothetical Ms. Sally Kaplan in Georgia could register and use the domain name "www.skaplan.com" to display pictures of her

grandchildren and to upload recipes. Stanley Kaplan testing service could at some point desire this domain name, and could seek to obtain it from Ms. Kaplan. Because her friends and family use this domain name to contact her, the domain name would be more valuable to Ms. Kaplan than the registration fees she had paid. Thus, she might ask Stanley Kaplan for an amount greater than what she originally paid to register the domain name. Under current decisional law, her use and "demand" could be considered cybersquatting and a violation of the FTDA. Clearly, the "noncommercial use" exception was meant to avoid this situation.

Courts have expanded the FTDA well beyond its tenuous borders by forcing the cybersquatting situation into trademark dilution. First, by granting relief to many companies that are not "famous," courts open the door for many companies to pursue dilution actions. This will not only overload the federal circuits, but will also create confusion concerning which marks can and should receive protection under the FTDA. Second, by expanding the definition of dilution to include not only tarnishment, but also to broaden the boundaries of "blurring," courts create incentives for companies to litigate any marginal dilution claim under the FTDA. Third, by expanding the "commercial use" requirement, courts threaten to chill many arguably non-commercial uses of trademarks. Thus, courts have effectively limited the communication value of words that correspond to trademarks by giving trademark owners excessive power over what can and cannot be said about their products and services.

III. CYBERSQUATTING IS BLACKMAIL

While several commentators have implied that cybersquatters are blackmailers or extortionists, this statement is usually made without further explanation.[64] No commentator has fully explored whether cybersquatting is consistent with blackmail.[65] Given the indefiniteness and flexibility in blackmail standards, this omission is surprising.

This section will explore various commentators' viewpoints on blackmail. The treatment of blackmail as a "paradox" is a common thread in these viewpoints. Blackmail is considered paradoxical because it often involves coupling the legally allowed disclosure of a secret with a threat to disclose unless payment is received.[66] Other commentators look at blackmail as a paradox because of its means/end connection.[67] For example, Professor Fletcher poses the following query: "Why should an innocent end (silence) coupled with a generally respectable means (monetary payment) constitute a crime?"[68]

Before looking at these differing viewpoints, an explanation of some types of blackmail is necessary. Scholars have divided blackmail into four categories, according to how the information is acquired.[69] "Participant blackmail" occurs when the blackmail stems from a prior relationship between the blackmailer and the blackmail victim.[70] "Opportunistic blackmail" occurs when the blackmailer serendipitously acquires the information.[71] "Commercial research blackmail" occurs when the blackmailer specifically conducts research in order to blackmail the victim.[72] Finally, "entrepreneurial blackmail" occurs when the blackmailer entraps the victim into a compromising situation in order to blackmail the victim.[73] Cybersquatting can best be described as commercial research blackmail since the cybersquatter "researches" and registers those domain names corresponding to popular trademarks.[74]

A. Theories of Blackmail

An influential rationale for criminalizing blackmail is that blackmail is economically wasteful, and should therefore be discouraged.[75] According to this view, the blackmailer uses valuable resources to collect information for the wasteful purpose of seeking payment to restrict the information's disclosure.[76] A related argument is that blackmail does not occur when the price asked is the "market price" for the information.[77] Both of these arguments are based on blackmail's economic impact.

The following commentators, Professors Epstein, Lindgren, Fletcher, and Gordon, disagree about which forms of blackmail should be illegal and about the cost-benefits of criminalizing blackmail. Either because of blackmail's moral implications or its economic waste, the commentators all agree that blackmail is wrong. These theories provide a background for determining the applicability of a blackmail standard to cybersquatting.

Professor Epstein suggests that blackmail is an exception to the general proposition that "where a person has the right to do a certain act . . . he has a right to threaten to do that act."[78] Epstein recognizes that legalizing blackmail may provide some benefits; private "moral" enforcement could provide incentives for people to reform unacceptable behavior.[79] Regardless of whether these benefits actually occur, blackmail leads to cooperation between the blackmailer and the blackmail victim to continue deceiving those who would be most benefited by the disclosure.[80] Because it breeds and sustains corruption and deceit, Epstein believes that blackmail should be illegal.[81]

Professor Lindgren faults conventional theories of blackmail for one of two reasons.[82] First, explanations that attack only a single part of the transaction cannot adequately distinguish why that part can be legitimate in some cases, but illegal in the blackmail situation.[83] Second, explanations that criminalize blackmail because of the harms that it causes cannot distinguish blackmail from other legal behaviors that cause the same harms.[84] To overcome these shortcomings, Lindgren emphasizes that blackmail's illegality is inherent in its "triangular nature" and because the blackmailer is using "someone else's leverage or bargaining chips" to threaten the blackmail victim.[85]

Professor Fletcher faults conventional theories for failing to distinguish adequately between lawful threats and illegal threats (i.e., blackmail).[86] Fletcher dismisses views that distinguish blackmail from lawful behavior solely because blackmail involves threatening to disclose information.[87] Fletcher also dismisses the distinction that German law makes between threats seeking property (e.g., money) as payment from those that seek sexual favors as payment.[88] Moreover, Fletcher argues that a theoretical distinction between "threats" and "offers" is unmanageable, because the two concepts are intractably dependent on context and norms.[89] Finally, while acknowledging the influence of Lindgren's paradigm of "playing with someone else's chips," Fletcher faults Lindgren for failing to fully develop this theory.[90]

Instead of reworking any pre-existing theory, Fletcher proposes a test that focuses on the dominance/subordination inherent in the blackmailer/blackmail victim relationship.[91] The

lynchpin of Fletcher's theory is the blackmailer's power to make repeated demands of payment.[92] Accordingly, Fletcher finds no blackmail in the controversial case of a homeowner's demand for payment in exchange for refraining from building a wall to such a height that it would block a neighbor's view.[93]

Unlike the aforementioned commentators, Professor Gordon does not seek to justify a perfectly encompassing definition of blackmail. On the contrary, Gordon suggests that no definition will include all possible situations of illegal threatening behavior without including any situation of legitimate threats.[94] Gordon focuses on why at least "central case" blackmail should be illegal under both consequentialist and non-consequentialist theories.[95] Central case blackmail "is where the blackmailer acquires information *for the sole purpose of obtaining money or other advantage from the victim*, and *where he has no intent or desire to publish the information, except as an instrument toward this purpose*."[96] Although Gordon only tackles the blackmail that most commentators agree should be illegal,[97] the breadth and strength of her explanation provides a useful definitional and analytical framework for blackmail.

Gordon presents a strong case for criminalizing central case blackmail for economic, or "consequentialist" reasons.[98] In central case blackmail, the disclosure "has no independent value to the seller," and if it were not prohibited, the victim would probably pay the price for silence.[99] This wastes resources without improving their allocation, and therefore, should be avoided.[100] Second, although legalizing central case blackmail might provide positive allocative effects,[101] these benefits would likely be outweighed by its harms.[102] In addition, legal central case blackmail would probably only deter nonconforming, though harmless, behavior; thus, its positive effects are likely to be minimal.[103] Finally, "wealth effects" may prevent blackmail transactions from directing resources to their highest valued uses.[104]

Notwithstanding her persuasive economic, or consequentalist arguments, Gordon's strongest argument for criminalizing central case blackmail is morality based, or non-consequential. In central case blackmail, the blackmailer "deliberately seeks to harm another to serve her own ends."[105] This harm is unjustified,[106] even if the blackmailer does not violate any property right of the victim.[107]

B. Applying Blackmail Theories to Cybersquatting

Epstein's view of blackmail does not coincide with cybersquatting.[108] His view requires either direct or indirect cooperation between the blackmailer and the blackmail victim to maintain the status quo (i.e., to keep the information secret). In cybersquatting, there is no cooperation between the cybersquatter and the trademark owner. In fact, the situation is more correctly described as antagonistic—the trademark owner would rather not negotiate with the cybersquatter. In addition, the trademark owner does not benefit from the status quo (i.e., the cybersquatter's retention of the domain name). This is exactly the harm that the trademark owner wants to prevent. Under Epstein's view, cybersquatting would more likely be considered a legal commercial threat.[109]

Applying Fletcher's view of blackmail to cybersquatting is also problematic. Fletcher's definition of dominance requires the possibility of repeat demands by the blackmailer.[110] In cybersquatting, the cybersquatter demands money from the legitimate trademark holder. Once the trademark holder pays the demand, however, the cybersquatter releases the domain name to the trademark holder and relinquishes the cybersquatter's leverage.[111] Under Fletcher's definition, this transaction would be legitimate because the "payment effects a settlement and thus negates the possibility of repeated demands."[112]

In contrast to Epstein and Fletcher's views, Lindgren and Gordon's definitions support a blackmail standard for cybersquatting. Lindgren suggests that blackmail occurs when the blackmailer uses someone else's "chips," or leverage, to extract what he desires from his victim.[113] Like the blackmailer, the cybersquatter uses someone else's leverage to extract money. The cybersquatter's "chip" is the goodwill that is associated with the mark, which legitimately belongs to the trademark holder and her customers.[114] Thus, Lindgren's view applies in that the cybersquatter uses the trademark holder and her customers' goodwill to extract money from the trademark holder.

Gordon's definition of central case blackmail also applies to cybersquatting. With slight modification, Gordon's definition of central case blackmail provides a useful definition of actionable cybersquatting for use by courts and/or legislatures. As stated above, in central case blackmail, the blackmailer acquires *information* solely to "obtain money or other advantage from the victim," with "no intent or desire to *publish the information*," except to gain an advantage.[115] Similarly, an illegal cybersquatter should be one who acquires a *domain name* for the sole purpose of obtaining money or other advantage from the *trademark owner*, with no intent or desire to *use the domain name*, except as an instrument toward this purpose. This definition would also complement Lindgren's view of blackmail. The domain name, or more correctly, the goodwill associated with the trademark corresponding to that domain name, belongs to others; the trademark owner and her customers.

This suggested definition fits nicely with cybersquatting cases. For example, the cybersquatter places no independent value in the registered domain name because his only goal is to receive payment from the trademark owner.[116] Because the cybersquatter receives no independent value from holding onto the domain name, cybersquatting fits the definition of central case blackmail.[117] Thus, the full force of Gordon's consequentialist and nonconsequentialist arguments could be applied to condemn cybersquatting behavior without stretching the FTDA to encompass cybersquatting.

Deciding cybersquatting cases under blackmail principles according to this suggested definition would also provide benefits that are unavailable under the FTDA. First, all trademark owners blackmailed by cybersquatters, even owners of non-"famous" marks, could pursue relief from cybersquatters. Because the FTDA limits its coverage to "famous" marks, owners of non-"famous" marks cannot presently receive protection.[118] Second, applying blackmail principles to cybersquatting would protect both innocent registrants and concurrent users. Because these users are not "blackmailing" trademark owners, the use of domain names that incidentally correspond to trademarks would not be actionable. Ownership of these domain names would be resolved through the bargaining process, not the judicial process. Thus, trademark owners would have to negotiate a fair price for the right to use a domain name that

had been registered by an earlier party.[119]

Central case blackmail principles would not, however, capture the questionable behavior of competitor grabbers, because competitor grabbers can receive independent value from the domain name. For example, competitor grabbers can increase their sales either by selling competing goods on the site, or by frustrating the trademark owner's customers by warehousing the site. Although this behavior is not central case blackmail, it may nonetheless constitute blackmail. This behavior, however, could probably be litigated under unfair competition principles.[120]

One problem courts would face in applying blackmail legislation to cybersquatting is choosing which state's blackmail law to apply. By modifying Gordon's definition of central case blackmail to encompass the cybersquatting situation, however, such a choice may not be necessary. Because central case blackmail is the least controversial type of blackmail, most states treat it similarly.[121] Thus, the forum shopping tactics that plague other choice of law cases may be reduced here.[122]

Courts in cybersquatting cases are also faced with the issue of personal jurisdiction. Because use of a website may affect people throughout the country, and even the world, plaintiffs may have difficulty knowing where to bring their cybersquatting claims. This procedural challenge, however, is not unique to victims of cybersquatting. Personal jurisdiction law for disputes involving all kinds of Internet transactions is currently unresolved.[123] Thus, Congress should adopt legislation to resolve personal jurisdiction disputes as well as establish the applicable choice of law concerning Internet disputes.

Although cybersquatting fits within the blackmail framework, the criminal punishment corresponding to blackmail should not necessarily apply to cybersquatting.[124] Criminal punishment has at least two general purposes: to act as a deterrent and to provide retribution.[125] Criminal punishment of cybersquatting would probably be effective as a general deterrent, because others would be less inclined to cybersquat for fear of criminal sanctions.[126] Criminal punishment may also provide a specific deterrent, because it would severely limit the cybersquatter's access to the Internet and to money, both of which are required to register a domain name.

The main problem with applying criminal sanctions to cybersquatters, however, is that such punishment is probably too harsh. Although cybersquatting is arguably a crime against society,[127] the real and direct injury is against the trademark owner. Trademark infringement is an aspect of unfair competition, which is a tort, not a crime.[128] Therefore, sanctions against cybersquatters should be handled through civil, not criminal sanctions.

A better solution would to be to establish a blacklist of cybersquatters. NSI could create a policy that punishes anyone found by a court to have cybersquatted.[129] This punishment could include losing all domain name registrations, including those not under adjudication. Such a sanction would prevent "adjudicated" cybersquatters from repeating their actions and remove any benefits the cybersquatter could have received from having access to the Internet. Because full access to the Internet is a valuable commodity, such a sanction might provide an effective deterrent to other would-be cybersquatters.

This sanction potentially raises First Amendment issues because it prohibits individuals

from expressing themselves through an important means of communication.[130] The breadth of First Amendment rights on the Internet has yet to be decided by the Supreme Court.[131] Only individuals that were found by trial to have committed cybersquatting would be blacklisted. However, because cybersquatters would be granted due process, and because their actions abuse the means of communication from which they would be restricted (by preventing others from effectively using the same means of communication), the cybersquatter's First Amendment claims would be weak.

IV. CONCLUSIONS

Applying trademark dilution theory to cybersquatting may appear to be a simple remedy. The cure, however, might be worse than the disease. By applying dilution to cybersquatting cases, courts have expanded the FTDA beyond its intended scope.

The FTDA was enacted to help owners of "famous" marks protect their marks from the abuse of both large and small competitors. By using the FTDA against cybersquatters, courts have not only granted protection to owners of indisputably "famous" marks, they have also granted protection to owners of questionably "famous" marks. In addition, by expanding the "commercial use" requirement, courts have created precedents that permit trademark owners to encroach into noncommercial uses. This may ultimately chill any expression that incidentally uses a trademark.

Instead of trademark dilution, courts should apply blackmail principles to cybersquatting. Cybersquatting fits within Gordon's definition of central case blackmail. Accordingly, Gordon's consequentialist and nonconsequentialist arguments against central case blackmail apply to cybersquatters. These arguments are more relevant to cybersquatting and are more persuasive than those supported by dilution theory.

Applying blackmail principles to the cybersquatting situation may discourage some of the choice of laws "forum-shopping" surrounding Internet cases. More apparently, courts could address cybersquatting without stretching the already tenuous FTDA. In addition, these principles would protect innocent registrants and concurrent users by encouraging trademark owners to negotiate for the desired domain names rather than bring suit.

---

† B.S., 1993, Environmental Engineering, Massachusetts Institute of Technology; Ph.D., 1997, Ecology, Evolution, and Animal Behavior, University at Albany, State University of New York; J.D. (anticipated), 2000, Boston University School of Law.

[1] *See, e.g.*, John Budris, *One Island, One Schoolhouse, One Student*, BOSTON GLOBE, Dec. 28, 1998, at B1, B2 ("Peculiarities in the phone service make Internet access seem more a potholed road than an information superhighway.").

[2] *See* G. Peter Albert, Jr., *Right on the Mark: Defining the Nexus Between Trademarks and Internet Domain Names*, 15 J. MARSHALL J. COMPUTER & INFO. L. 277, 278 (1997).

[3] *See id.*

[4] *See id.* Initially the Internet's primary users were the government and universities. *See id.* This transformation from a military function to a primarily civilian function upon cessation of a military threat (i.e., the end of the Cold War) is similar to manufacturing companies' shift after World War I from primarily arms and munitions to

peacetime products. *See* Frank I. Schecter, *The Rational Basis of Trademark Protection*, 40 HARV. L. REV. 813, 823 (1927) (citing Remington Arms and DuPont as examples of companies that shifted their focus).

[5] *See* Albert, *supra* note 2, at 278 ("The diversification of Internet users, along with Web development, has caused a significant change of attitude regarding advertising and commercialization.").

[6] *See id.* at 278-79 (discussing the Web's contribution to e-commerce); *see also* Danielle W. Swartz, *The Limitations of Trademark Law in Addressing Domain Name Disputes*, 45 UCLA L. REV. 1487, 1489 (1998) ("[T] he easy accessibility and convenience of the Internet for consumers make cyberspace an invaluable environment for promoting and selling goods and services.").

[7] *See* Swartz, *supra* note 6, at 1488. A domain name is the user-friendly, alphanumeric equivalent of a unique numerical Internet Protocol address. *See id.* at 1490; Panavision Int'l, L.P. v. Toeppen, 945 F. Supp. 1296, 1299 (C.D. Cal. 1996) (explaining that every computer linked to the Internet is assigned a numeric address consisting of four sets of digits separated by periods (e.g., 171.26.4.28)).

[8] *See* Albert, *supra* note 2, at 280 ("NSI is responsible for the registration of domain names that have any one of six possible top levels . . . include[ing] '.com'.").

[9] *See* Gregg Duffey, Comment, *Trademark Dilution Under the Federal Trademark Dilution Act of 1995: You've Come a Long Way Baby – Too Far, Maybe?*, 39 S. TEX. L. REV. 133, 147 (1997) (noting that NSI issues domain names without considering trademark ownership).

[10] NSI stated that performing a trademark check for each domain name registration would cost thousands of dollars and unnecessarily delay the time it takes to successfully register a domain name. *See* Martin B. Schwimmer, *Domain Names and Everything Else: Trademark Issues in Cyberspace*, *in* UNDERSTANDING BASIC TRADEMARK LAW 1998, at 263, 269 (PLI Pat., Copyrights, Trademarks & Literary Prop. Course Handbook Series No. G0-0015, 1998). A standard trademark registration check costs only $245, including the filing fee. *See id*. Thus, it hard to see why NSI, an automated operation, would not be able to perform a trademark check for less money or time. *See id.* InterNIC, the agency responsible for overseeing NSI, has said that it would take twenty people to do trademark checks for domain names and that the responsibility should be on the registrant. *See* Neal J. Friedman & Kevin Siebert, *The Name Is Not Always the Same*, 20 SEATTLE U. L. REV. 631, 635-36 (1997) (citing InterNIC manager Scott Williamson).

[11] *See* Swartz, *supra* note 6, at 1494 (noting that ransom grabbers "strategically register trademarks as domain names . . . to sell to . . . trademark holders . . . ."). Other grabbers are competitors who register domain names either to offer their competing goods or just to hinder the trademark holder's use of the domain name. *See id*. at 1494-95. For purposes of this paper, cybersquatters will only include individuals who act as ransom grabbers.

[12] ICANN was formed in November 1998 as a non-profit, private sector corporation "to take over responsibility for the IP address space allocation, protocol parameter assignment, domain name system management, and root server system management functions . . . ." *About ICANN* (last modified Mar. 26, 2000) <http://www.icann.org/general/>. Before November 1998, the U.S. government contracted its domain name allocation services to NSI. *See* Albert, *supra* note 2, at 280.

[13] *See* Michael R. Gottfried & Anthony J. Fitzpatrick, *The Internet Domain Name Landscape in the Wake of the Government's "White Paper,"* BOSTON B.J., Nov.-Dec. 1998, at 8, 9.

[14] *See* ICANN, *Uniform Domain Name Dispute Resolution Policy* (last modified Jan. 3, 2000) <http://www.icann.org/udrp/udrp-policy-24oct99.htm> [hereinafter ICANN, *Policy*]. The Dispute Resolution Policy was adopted on August 26, 1999, and the implementing rules were approved on October 24, 1999. *See id.*; ICANN, *Rules for Uniform Domain Name Dispute Resolution Policy* (last modified Jan. 3, 2000) <http://www.icann.org/udrp/udrp-rule-24oct99.htm> [hereinafter ICANN, *Rules*]. These rules provide detail on

how and to whom a complaint should be filed, the format of the complaint, and the contents of the complaint. *See id*. ¶¶ 2-3. The rules also discuss, in detail, the review procedure and the interaction of the complaining and responding parties with the review panel. *See id.* ¶¶ 6-18.

[15] *See* ICANN, *Policy*, *supra* note 14, ¶ 4(i) ("The remedies available to a complainant pursuant to any proceeding before an Administrative Panel shall be limited to requiring the cancellation of your domain name or the transfer of your domain name registration to the complainant.").

[16] For example, the time to go through the ICANN arbitration procedure may cost the corporation more money in lost profits than the cybersquatter is asking for immediate transfer. Therefore, for pure business reasons, corporations may choose to pay a cybersquatter rather than enter into the ICANN arbitration procedure. Thus, a clever cybersquatter could find the right amount for a given corporation that they would choose to pay the cybersquatter rather than taking legal action.

For this reason, and possibly other less noble reasons, businesses pushed Congress to pass the Anticybersquatting Consumer Protection Act ("ACPA"), 15 U.S.C.A. § 1125 (d) (West Supp. 2000). The ACPA provides trademark holders a cause of action against bad faith registrants of their trademarked names. *See id.* § 1125 (d)(1)(A)(i). The ACPA further provides a successful plaintiff either actual damages and profits or statutory damages as high as $1,000,000. *See id*. §§ 1125(c)(2), 1117(c), 1118.

[17] The commercial aspects of the World Wide Web changed how businesses viewed the Internet and the Web's advertising potential greatly attracted commerce. *See* G. Gervaise Davis III, *Internet Domain Names and Trademarks: A Growing Area of Dispute*, *in* PLI'S THIRD ANNUAL INSTITUTE FOR INTELLECTUAL PROPERTY LAW, at 649, 656 (PLI Pat., Copyrights, Trademarks, & Literary Prop. Course Handbook Series No. G4-4008, 1997). Because cybersquatters target companies who can afford to pay a ransom for the domain name, cybersquatting was not a real problem until commercial businesses wanted to get on the Internet. *See id.* at 656, 659.

[18] Intermatic Inc. v. Toeppen, 947 F. Supp. 1227, 1233 (N.D. Ill. 1996).

[19] *See* Swartz, *supra* note 6, at 1494-95.

[20] *See id.*

[21] *See id*.

[22] Innocent users "innocently register a name that has particular meaning to them—such as their last name or the name of a loved one—that also happens to be someone else's registered trademark." *Id.* at 1495.

[23] *See id.*

[24] *See, e.g.*, Panavision Int'l, L.P. v. Toeppen, 945 F. Supp. 1296, 1303 (C.D. Cal. 1996) (stating that Toeppen's cybersquatting "conduct injured Panavision by preventing Panavision from exploiting its marks").

[25] *See* Swartz, *supra* note 6, at 1493 (stating that domain names "must be unique"); Schwimmer, *supra* note 10, at 266 ("[W]hile identical trademarks can co-exist in the marketplace, identical domain names cannot coexist on the Internet.").

[26] *Panavision*, 945 F. Supp. at 1300. Toeppen had applied and received registration from NSI for the domain name "www.panavision.com" in December of 1995, and Panavision brought suit in May of 1996. *See id.*

[27] *See id.* at 1303. Panavision chose to litigate against Toeppen even though it probably would have been cheaper

to pay the $13,000. *See id.* Toeppen had been counting on the fact that it would be cheaper for Panavision to pay the fee, as that is how Toeppen ran his domain-name "business." *See id.*

[28] As long as the desired domain name is different from one already registered, NSI would grant the registration. *See* Albert, *supra* note 2, at 281; s*ee also supra* notes 14-15 and accompanying text (discussing that the new ICANN-accredited registrars still distribute names without checking if a trademark holder might have a claim to the domain name).

[29] *See generally* Swartz, *supra* note 6, at 1491-92 ("Many businesses choose to use their trademarks as domain names because consumers are already familiar with those marks . . . . Internet users often guess that a product's trademark also serves as the domain name that accesses a website with information about the product."). Because of this preference, cybersquatters generally register a domain name that corresponds to the actual trademark. *See id.* at 1499-1500.

[30] *See id.* at 1492. Search engines search the Internet using key words. *See Panavision*, 945 F. Supp. at 1299. A typical search will often bring up thousands of webpages that use that key word, so that a customer seeking only a specific name must wade though this list to find the one site that has the information he is seeking. *See id.*

[31] A typical search engine will retrieve all domain names that contain the requested term, including any competitors' domain names, if the competitors compare or otherwise mention the trademark owner's products. In addition, because search engines generally retrieve any domain that uses the requested term, disclaimers may be ineffective for these searches. *See* Schwimmer, *supra* note 10, at 286-87 (discussing Playboy Enter., Inc. v. Terri Welles, 7 F. Supp. 2d 1098 (S.D. Cal. 1998)). In *Welles*, a former Playboy Playmate of the Year set up a webpage and disclaimed any association with PLAYBOY. *See id*. A search looking for 'playboy' would nonetheless retrieve this site. *See id.*

[32] *See supra* notes 29-30 and accompanying text.

[33] *See supra* note 31 and accompanying text.

[34] Some have questioned whether ordinary trademark infringement claims might prevail against cybersquatters. *See, e.g.*, Swartz, *supra* note 6, at 1496-1505. Traditional infringement tests may be ineffective because they are either over- or under-inclusive. This shortcoming is inherent in three critical factors: 1) similarity of the marks—innocent registrants and concurrent trademark holders could also have similar marks; 2) proximity of the goods—many cybersquatters do not advertise any goods on the desired domain name; and 3) marketing channels—many cybersquatters only warehouse the domain name and therefore do not use any marketing channels. Courts could also apply the same standards to the domain name problem as courts do to cases involving telephone mnemonics. *See* Albert, *supra* note 2, at 289-94, 307-08. Domain names are similar to telephone mnemonics in that they have to be unique, and case-law has already been established for deciding who infringes by using a similar or desired telephone mnemonic. *See id*. at 307-08. Therefore, courts could apply this caselaw to domain name disputes. *See id*. Unfortunately, there is a split in authority concerning telephone mnemonic cases. *See id*. Also, the telephone mnemonic cases rely on a likelihood of consumer confusion, an element that is usually lacking, or very hard to prove, in the cybersquatting situation. *See id.* at 292-93.

[35] This trend is probably due to the fact that all courts deciding cybersquatting cases have applied dilution theory. *See, e.g.*, Intermatic Inc. v. Toeppen, 947 F. Supp. 1227, 1239-41 (N.D. Ill. 1996); *Panavision*, 945 F. Supp. at 1301.

[36] Schechter, *supra* note 4.

[37] *See id.* at 819 ("The mark actually *sells* the goods. And, self-evidently, the more distinctive the mark, the more effective is its selling power.").

[38] *See id.* at 822 ("[T]he preservation of the uniqueness or individuality of the trademark is of paramount importance to its owner."); s*ee also* Rudolf Callmann, *Trade-mark Infringement and Unfair Competition*, LAW & CONTEMP. PROBS., Spring 1949, at 185, 189 (1949) (agreeing with Schechter that the property right inherent in trademark ownership should allow protection beyond merely protecting consumers from confusion). *But see* Ralph S. Brown, Jr., *Advertising and the Public Interest: Legal Protection of Trade Symbols*, 57 YALE L.J. 1165, 1205 (1948) (arguing that protection of a mark's intrinsic symbol value from dilution is not a desirable interest because it would grant the trademark owner a limited monopoly that he does not deserve; only the informational, reputational, and goodwill aspects of a trademark should be protected).

[39] *See* Malla Pollack, *Time to Dilute the Dilution Statute and What Not to Do When Opposing Legislation*, 78 J. PAT. & TRADEMARK OFF. SOC'Y 519, 520 (1996) (arguing that dilution is concerned not with protecting consumers, but with protecting the property interests of trademark owners).

[40] *See* Federal Trademark Dilution Act of 1995, 15 U.S.C. §§ 1125, 1127 (1994 & Supp. IV 1999).

[41] State statutes generally required plaintiffs to establish "(1) a distinctive mark and (2) a likelihood of dilution." Duffey, *supra* note 9, at 140. The federal dilution statute arguably eliminated some of the major problems that faced plaintiffs seeking dilution protection from the various states. *See id*. at 141. One problem was the uncertain ability of state courts to grant extraterritorial injunctions (i.e., injunctions that involved uses of similar marks beyond the state boundaries). *See id*. Another problem was the lack of uniformity of state courts in handling dilution questions, which encouraged forum shopping. *See id.*

[42] *See* 15 U.S.C. § 1125(c)(1) ("The owner of a *famous* mark shall be entitled [to relief under this section] . . . .") (emphasis added).

[43] The FTDA provides:

> In determining whether a mark is distinctive and famous, a court may consider factors such as, but not limited to–
>
> (A) the degree of inherent or acquired distinctiveness of the mark;
> (B) the duration and extent of use of the mark in connection with the goods or services with which the mark is used;
> (C) the duration and extent of advertising and publicity of the mark;
> (D) the geographical extent of the trading area in which the mark is used;
> (E) the channels of trade for the goods or services with which the mark is used;
> (F) the degree of recognition of the mark in the trading areas and channels of trade used by the marks' owner and the person against whom the injunction is sought;
> (G) the nature and extent of use of the same or similar marks by third parties; and
> (H) whether the mark was registered under the Act of March 3, 1881, or the Act of February 20, 1905, or on the principal register.

Id.

[44] *See id.* § 1125(c)(1)-(4).

[45] *See, e.g.*, Mead Data Cent., Inc. v. Toyota Motor Sales, U.S.A., Inc., 875 F.2d 1026, 1028 (2d Cir. 1989) (holding that LEXIS is a strong mark, not because it is arbitrary, but because Mead had extensive sales and advertising of the LEXIS mark; no dilution relief because its fame is limited to one percent of the population); Kraft General Foods, Inc. v. Allied Old English, Inc. 831 F. Supp. 123, 134 (S.D.N.Y. 1993) (citing Judge Sweet's concurrence in *Mead Data* and holding that to warrant dilution relief, Bulls-Eye barbecue sauce did not need to be "famous" or "celebrated," it must merely be an extremely strong mark either through inherent distinction or through acquiring secondary meaning).

[46] *See, e.g.*, Panavision Int'l, L.P. v. Toeppen, 945 F. Supp. 1296, 1298 (C.D. Cal. 1996) (involving claims brought by Panavision for federal (FTDA) and state (California) trademark dilution, federal trademark infringement,

and federal unfair competition); Intermatic Inc. v. Toeppen, 947 F. Supp. 1227, 1229 (N.D. Ill. 1996) (involving claims brought by Intermatic for federal (FTDA) and state (Illinois) trademark dilution, federal trademark infringement, federal unfair competition, common law unfair competition, and state deceptive trade practices).

[47] *See, e.g.*, *Panavision*, 945 F. Supp. at 1304 (stating that since Panavision prevailed on federal and state dilution claims, "it is unnecessary . . . to reach the issues of federal and state trademark infringement and federal unfair competition."). Of course, courts may also feel justified in applying the FTDA aggressively against cybersquatters. *See* 141 CONG. REC. S19312 (daily ed. Dec. 29, 1995) (statement of Sen. Leahy) (hoping that passing the FTDA would "help stem the use of deceptive Internet addresses taken by those who are choosing marks that are associated with the products and reputations of others.").

[48] *See supra* notes 42-44 and accompanying text.

[49] *See Panavision*, 945 F. Supp. at 1302-03 (holding that Panavision is a famous mark because of federal registration, extensive advertising, and development of strong secondary meaning).

[50] *See Intermatic*, 947 F. Supp. at 1239 (holding that Intermatic is "famous" as a matter of law because it "is a strong fanciful federally registered mark, which has been exclusively used by Intermatic for over 50 years.").

[51] *See* TeleTech Customer Care Mgmt., Inc. v. Tele-Tech Co., Inc., 977 F. Supp. 1407, 1411 (C.D. Cal. 1997) (finding that the plaintiff could probably prove it held a "famous" mark).

[52] *See* Schwimmer, *supra* note 10, at 276-77 (noting that decisions granting "famous" marks protection beg the question, "[i]s it possible that in the rush to prevent domain name piracy, dilution law has been diluted?").

[53] *See Teletech*, 977 F. Supp. at 1412 (granting preliminary injunction because the mark was likely to succeed on the merits of its dilution claim); *Intermatic*, 947 F. Supp. at 1240 (finding it likely that Toeppen's use of the domain name would cause dilution of Intermatic's famous mark).

[54] 15 U.S.C. § 1125(c) (Supp. IV 1999).

[55] *See* Robert C. Denicola, *Some Thoughts on the Dynamics of Federal Trademark Legislation and the Trademark Dilution Act of 1995*, LAW & CONTEMP. PROBS., Spring 1996, at 75, 88-89. Although the dilution proposal for the 1988 amendments contained a provision to protect trademark owners from tarnishment, the 1995 Act purposely does not. *See id*. The Trademark Review Commission report states that the injury from tarnishment is "less dilution than injury to reputation[]" and does not fit conceptually with dilution. U.S. Trademark Ass'n, Trademark, Review Comm'n, *Report and Recommendations to USTA President and Board of Directors*, 77 TRADEMARK REP. 375, 434 (1987). Nonetheless, courts have used the FTDA to protect trademark holders from tarnishment by others on the Internet. *See, e.g.*, Toys "R" Us, Inc. v. Akkaoui, No. C96-3381CW, 1996 WL 772709, at *4 (N.D. Cal. Oct. 26, 1996) (enjoining adult site owner from using site "www.adultsrus.com"); Hasbro, Inc. v. Internet Entertainment Group, Ltd., No. C96-130WD, 1996 WL 84853, at *1 (W.D. Wash. Feb. 9, 1996) (enjoining adult site user from using domain name "www.candyland.com"). The problematic use of the FTDA to claim tarnishment is not limited to Internet cases. *See* Hormel Foods Corp. v. Jim Henson Prod., Inc., 73 F.3d 497 (2d Cir. 1996) (holding that although there was no tarnishment in the instant case, tarnishment was a valid cause under dilution statutes). Although *Hormel Foods* was not decided under the FTDA, it was decided only two weeks before the FTDA was signed into law, and demonstrates concurrent judicial interpretation.

[56] *Intermatic*, 947 F. Supp. at 1240; s*ee also* Daniel R. Pote, *A Domain by Any Other Name: The Federal Trademark Dilution Act of 1995 Applied to Internet Domain Names*, 37 JURIMETRICS J. 301, 314-15 (1997) (citing Panavision Int'l, L.P. v. Toeppen, 945 F. Supp. 1296, 1303 (C.D. Cal. 1996)).

[57] *See, e.g.*, Pollack, *supra* note 39, at 526-27 ("The dilution statute will probably fuel more cases barring counter-

cultural or political protest use of well-known communication symbols."). Many such symbols may legitimately belong in the public domain; their restriction raises First Amendment concerns. *See id*. at 527.

[58] *See* 947 F. Supp. 1296, 1232 (C.D. Cal. 1996).

[59] *See id.* at 1239. *But see* Cardservice Int'l, Inc. v. McGee, 950 F. Supp. 737, 741 (E.D. Va. 1997) ("[A] domain name is more than a mere Internet address. It also identifies the Internet site to those who reach it, much like . . . a company's name identifies a specific company.").

[60] *Intermatic*, 947 F. Supp. at 1239; *see also Panavision*, 945 F. Supp. at 1303 (holding that Toeppen's use of the domain name was commercial).

[61] *See* 15 U.S.C. § 1125(c)(4) (Supp. IV 1999) ("The following shall not be actionable under this section: (A) Fair use . . . in comparative commercial advertising . . . (B) Noncommercial use of a mark. (C) All forms of news reporting and news commentary."); s*ee also* Avery Dennison Corp. v. Sumpton, 999 F. Supp. 1337, 1340-41 (C.D. Cal. 1998) (noting that cybersquatters who registered many domain names corresponding to popular surnames in order to resell to individuals who would want to use one of these domain names as an email address violated the FTDA). *But see* Albert, *supra* note 2, at 303-04 (arguing that cybersquatters that only used domain names as e-mail addresses would be abusing the noncommercial use exception and thus their conduct should be actionable and prevented by the FTDA).

[62] 4 J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS § 25:77, at 25-153 n.9 (1999) (internal citations omitted).

[63] *See* Denicola, *supra* note 55, at 91 (arguing that Congress intended courts to broadly interpret the "noncommercial use" exception of the FTDA).

[64] *See e.g.*, Davis, *supra* note 17, at 660 (stating that cybersquatting behavior "dangerously border[s] on extortion . . . ."); Friedman & Siebert, *supra* note 10, at 644-45 (calling cybersquatting a form of domain name blackmail).

[65] Blackmail is succinctly defined as a special case of extortion where the threat is to disclose information rather than to inflict physical harm. *See* James Lindgren, *Unraveling the Paradox of Blackmail*, 84 COLUM. L. REV. 670, 674 (1984).

[66] *See id.* at 670-71 ("In blackmail, the heart of the problem is that two separate acts, each of which is a moral and legal right, can combine to make a moral and legal wrong."); Richard A. Epstein, *Blackmail Inc.*, 50 U. CHI. L. REV. 553, 557 (1983) (arguing that blackmail is an anomalous exception to the general rule that "where a person *has* the right to do a certain act . . . he has the right to threaten to do that act.").

[67] *See* George P. Fletcher, *Blackmail: The Paradigmatic Crime*, 141 U. PA. L. REV. 1617, 1617 (1993).

[68] *Id.* Fletcher goes on to say that this "paradox" is not unique to blackmail, but is also relevant for crimes such as bribery and prostitution. *See id. But see* Wendy J. Gordon, *Truth and Consequences: The Force of Blackmail's Central Case*, 141 U. PA. L. REV. 1741, 1743-45 (1993). Because a person might not have a right to threaten to do an act, even if he has the right to actually do the act, there is no paradox. *See id*.

[69] *See* Mitchell N. Berman, *The Evidentiary Theory of Blackmail: Taking Motives Into Account*, 65 U. CHI. L. REV. 795, 803 (citing MICHAEL HEPWORTH, BLACKMAIL: PUBLICITY AND SECRECY IN EVERYDAY LIFE 73-77 (1975)).

[70] An example of participant blackmail is when a woman in an adulterous affair with a married man threatens to disclose this affair to the man's wife unless he financially provides for her. *See* Berman, *supra* note 69, at 803.

[71] An example of opportunistic blackmail is when a person sitting in his apartment overhears a loud conversation between a married man and his mistress, and he then demands money from the married man not to disclose this information to the man's wife. *See id*.

[72] An example of commercial research blackmail is when a person suspects that an accused tax-evader bribed a judge, researches the situation to determine if it is true or not, and then demands money from the judge not to disclose his findings to the press. *See id*.

[73] For example, when a gossip magazine paid a woman to seduce Gifford and bring him to a hotel room, the magazine had wired the room in order to take pictures of the affair, the magazine would have engaged in entrepreneurial blackmail if it had threatened to publish the pictures unless Gifford paid the magazine a sum of money. *See id.*

[74] Of course, the cybersquatter may have to perform very little research since many trademark owners (through advertising or goodwill) have made their trademarks part of the common vocabulary. For instance, it is unlikely that Toeppen had to do much (if any) research to discover that Panavision would want to own the domain name "www.panavision.com." *See* Panavision Int'l, L.P. v. Toeppen, 945 F. Supp. 1296 (C.D. Cal. 1996).

[75] *See* William M. Landes & Richard A. Posner, *The Private Enforcement of Law*, 4 J. LEGAL STUD. 1, 42-43 (1975) (arguing that private enforcement of moral standards by blackmailers is forbidden because it is economically wasteful); *but see* Fletcher, *supra* note 67, at 1618 (arguing that criminalizing blackmail solely because of its inefficiency is unpersuasive, since many other inefficient activities are legal); s*ee also* ROBERT NOZICK, ANARCHY, STATE, AND UTOPIA 84-86 (1974) (arguing that market-price blackmail may at times be a productive exchange and as such should not be prohibited in some situations). *But see* Lindgren, *supra* note 65, at 707 (arguing that if the blackmailer uses someone else's leverage, it should be illegal even if the exchange is productive).

[76] Usually the blackmailer must spend time or money to collect enough information to pose a threat to the blackmail victim. Of course, the blackmailer may have been merely a bystander to a private conversation or act that the blackmail victim would not want disclosed. *See supra* note 71 and accompanying text (defining "opportunistic blackmail"). Still, the blackmail itself is merely a transfer of resources that does not improve the allocation of economic resources. Thus, even "bystander blackmail" is economically inefficient.

[77] The "market price" for blackmail is established if there is more than one buyer (e.g., the person who wants the information kept secret and a newspaper that wants to publish the information). Multiple buyers create a market where a "fair" economic price may be established. *See* Nozick, *supra* note 75, at 85-86 (arguing that market-price blackmail should be allowed for use against public individuals); Jeffrie G. Murphy, *Blackmail: A Preliminary Inquiry*, 63 MONIST 156, 164-65 (1980) (arguing that market-price blackmail should be allowed for blackmail of public individuals but not for blackmail of private individuals).

[78] Epstein, *supra* note 66, at 557; *see also* Landry v. Daley, 280 F. Supp. 938, 961 (N.D. Ill. 1968) *rev'd on other grounds sub nom.* Boyle v. Landry, 401 U.S. 77 (1971) (refusing to apply an Illinois blackmail statute where the defendant threatened to commit the act which he had a legitimate right to commit). *But see* Gordon, *Truth and Consequences, supra* note 70, at 1744 (arguing that even if a person has the right to act in a certain way, he may not have a right to threaten to do so since threats and acts may cause significantly different harms).

[79] *See* Epstein, *supra* note 68, at 561-62 ("[I]ndividuals are less likely to engage in illegal practices if they know that wholly apart from criminal sanctions they face the risk of monetary payments as well."); *see also* Landes & Posner, *supra* note 75, at 42 (arguing that private "moral" enforcement in some situations does not lead to over-enforcement; consequently, such private enforcement should not be considered blackmail). *But see* Gordon, *supra*

note 68, at 1766 (“Since the blackmailer’s end is harm, the act is not redeemable by the possibility that some component of the means he uses might be lawful or beneficial.”).

[80] For example, a blackmailer could instruct the blackmail victim on how to maintain the secret for their mutual benefit in order to best guarantee an income stream for the blackmailer and best guarantee secrecy for the blackmail victim. *See* Epstein, *supra* note 66, at 564.

[81] “Blackmail should be a criminal offense . . . because it is the hand-maiden to corruption and deceit.” *Id*. at 566.

[82] *See* Lindgren, *supra* note 65, at 672.

[83] *See generally id.* at 680-89. Theories that attempt to distinguish between moral and immoral liberties fail to show why the threat to take some types of moral liberties, but not others, is considered blackmail. *See id.* at 680-82. Theories that would sanction any conduct that promotes a lawful business fail to show why it is blackmail to threaten to publish true stories about an individual unless the individual purchases advertisements in the newspaper, even though such a threat serves to promote a lawful business. *See id*. at 682-83. Theories that attempt to make concealment wrongful are over-inclusive, since many of the lawful activities of private detectives, security firms, and lawyers would be prohibited. *See id*. at 684-87. Theories that would criminalize the sale of private information are also over-inclusive because sometimes there are legitimate transactions in private information. *See id.* at 687-89.

[84] *See generally id.* at 689-700. Theories that focus on blackmail’s invasion of privacy “cannot explain participant or opportunistic blackmail.” *Id*. at 690. Theories that would criminalize blackmail because it provides incentives to uncover information fail because they do not “explain participant or opportunistic blackmail,” and they would criminalize many legitimate bargaining situations. *See id*. at 694-97. Theories that focus on blackmail’s creation of private enforcement fail because they cannot explain why blackmail should be illegal when it enforces moral customs while more conventional private enforcement (e.g., firing, never hiring, refusing to negotiate) should be legal. *See id.* at 697-99. Theories that would criminalize blackmail because it is an unproductive exchange fail because it cannot explain why other instances of unproductive exchanges are not illegal. *See id*. at 699-700.

[85] *Id*. at 702. The blackmailer parasitizes an actual or potential dispute between two parties “in which he lacks a sufficiently direct interest.” *Id.*

[86] *See* Fletcher, *supra* note 67, at 1618-21.

[87] *See id.* at 1620 (explaining that no principled distinction exists explaining blackmail by mode of behavior (i.e., threatening to disclose information)).

[88] *See id.* (arguing that to focus on the differences between property and non-property results in placing too much attention on the ends sought, and not on the “criminal” means used).

[89] *See id.* at 1621-24 (requiring an unknowable “baseline of normalcy” to characterize any particular situation as a threat or an offer); *cf*. Wendy J. Gordon, *Of Harms and Benefits: Torts, Restitution, and Intellectual Property*, 21 J. LEGAL STUD. 449, 451 (1992) (arguing that to distinguish between harms and benefits requires determination of the “proper” baseline).

[90] *See* Fletcher, *supra* note 67, at 1624-25 (stating that under Lindgren’s view, any windfall profits made from bargaining with another’s chip should be criminal; thus, shrewd business persons would be committing blackmail for taking advantage of excess consumer surplus).

[91] *See id*. at 1626 (“The proper test . . . is whether the transaction with the suspected blackmailer generates a relationship of dominance and subordination.”).

[92] For example, since payment of a demand for the settlement of a tort dispute ends the transaction, there is no blackmail because there is no possibility for repeated demands. *See id.*

[93] *See id*. at 1628. Building the wall is within the homeowner's domain of freedom, so there is no domination of the neighbor. *See id.* at 1628. If the homeowner gains nothing from a higher fence, however, the threat is merely gratuitous. Accordingly, the threat would be blackmail in jurisdictions that follow the Model Penal Code. *See* MODEL PENAL CODE § 223.4 (1980) (prohibiting threats "to inflict any harm that would not benefit the actor"). *But see* Lindgren, supra note 65, at 679, 711-12 (arguing that this provision could possibly prohibit many legitimate bargaining tactics).

[94] *See* Gordon, *supra* note 68, at 1742 (noting that a synthesis of "consequentialist" and "nonconsequentialist" theories is required to explain the most complex situations).

[95] *See id*.

[96] *Id.* at 1746 (emphasis in original). This definition is similar to the notion of "commercial research blackmail." *See supra* note 72.

[97] *See* Gordon, *supra* note 68, at 1746 ("'[C]entral case' [blackmail] . . . should inspire the most agreement.").

[98] *See generally id.* at 1748-57.

[99] *Id.* at 1749.

[100] The proposition realistically assumes that there are positive transaction costs. *See id.* at 1749-50. Although blackmail may not improve resource allocation, nonallocativity is insufficient to criminalize blackmail. *See id. But see* Nozick, *supra* note 75, at 84-86 (arguing that because blackmail is an unproductive exchange, blackmail should be illegal).

[101] Nonconformists may be induced to change their behavior if they are forced to make blackmail payments. *See* Gordon, *supra* note 68, at 1753 n.64; Landes & Posner, *supra* note 75, at 42-43.

[102] The increased transaction costs from "silence-yielding (nonallocative) transactions" might outweigh any potential benefits from inducing more acceptable behavior. Gordon, *supra* note 68, at 1752.

[103] "[S]ociety already makes harmless and nonconforming behavior too expensive." *Id.* at 1753 n.64.

[104] If reputation is a fundamental resource (i.e., one associated with strong wealth effects) then the final owner may vary with the law's original assignment of entitlements. *See id.* at 1755-56. "Where the highest valued use is known, usual economic wisdom suggests the resource should be initially assigned to that use." *Id*. at 1756 n.73.

[105] *Id.* at 1758. Because the blackmailer intends to harm his victim, the blackmailer should be subject to the full force of the nonconsequential view. *See id.* at 1762.

[106] "[I]t is wrong to treat another as a means rather than as an end in himself[.]" *Id.* at 1760. Some have argued that because the blackmail victim has done something of which society disapproves, the blackmail victim deserves little protection. *See* Murphy, *supra* note 77, at 162. This argument is weakened by the fact that the blackmailer actively assists the blackmail victim in deceiving society, and profits by using society's chip. *See* Lindgren, *supra* note 65, at 702. In addition, Gordon suggests that the blackmail victim's rights should be defined as "a right to be free from the harm that the [blackmailer] intended and imposed. The harm intended and imposed . . . is not to [the

victim's] reputation; it is harm to the victim's pocketbook or to her liberty." Gordon, *supra* note 68, at 1769.

[107] Harm need not be limited to property rights; thus, harm to someone's reputation may be actionable. *See id*. at 1766-67. Also, the harm intended by the blackmailer may be viewed as harm to the blackmail victim's "property rights." *See supra* note 104 and accompanying text.

[108] In a blackmail situation both participants desire to keep the information secret (i.e., maintain the status quo) since they both benefit from its secrecy and would lose at least this benefit (and possibly more) if the information were disclosed). *See* Epstein, *supra* note 66, at 565.

[109] A seller can threaten not to sell to the purchaser unless a certain price is paid, and can legitimately remove the offer if the price is not paid. *See id.* at 557. If the cybersquatter has no right to the domain name in the first place, however, the threat may not occur in the context of a legitimate commercial transaction.

[110] "The dominance consists in the knowledge that the victim is now fair game for repeated demands." Fletcher, *supra* note 67, at 1638.

[111] Of course, a cybersquatter could conceivably register multiple domain names that one trademark holder desires and could legitimately claim. For example, the cybersquatter might register both "www.ringlingbrothers.com" and "www.the.greatest.show.on.earth.com". Ringling Brothers may desire these domain names because the corporation has trademarks corresponding to both. Thus, even if the registrant received payment for and released one domain name, the registrant could still make a demand for the other domain name. Under Fletcher's definition, however, this would be considered two separate transactions even though the parties and the subject matter are the same.

[112] Fletcher, *supra* note 67, at 1637. Fletcher distinguishes between non-punishable threats and punishable blackmail by the repeatability of the threats. *See id.* ("Conversely, all the cases of punishable blackmail generate a situation that invites repeated threats and exploitation.").

[113] *See* Lindgren, *supra* note 65, at 702.

[114] "Good will is a business value that reflects the basic human propensity to continue doing business with a seller who has offered goods and services that the customer likes and has found adequate to fulfill his needs." 1 MCCARTHY, *supra* note 62, § 2:17 at 2-37. As such, both the consumer and trademark owner benefit from the goodwill associated with a mark.

[115] Gordon, *supra* note 68, at 1746.

[116] Cybersquatters have "no intention of ever using [domain names] for any purpose other than to seek payment from the legitimate owners of the rights in the marks and names." Gottfried & Fitzpatrick, *supra* note 13, at 9.

[117] *See* Gordon, *supra* note 68, at 1752 n.62.

[118] *See supra* notes 42-45, 48-53 and accompanying text.

[119] This exchange could be productive in a number of ways. First, the trademark owner could negotiate to purchase the domain name. The innocent registrant or concurrent user could then ask the trademark owner what value she places on the domain name. Through successful negotiation, the party that places a higher value on the domain name should end up with the domain name. As there is no blackmail involved, this negotiation should not be hampered. Second, the trademark owner could offer to purchase advertising on the innocent registrant's or concurrent user's site. This would benefit both parties to the transaction—the trademark owner would channel

Internet users who guessed at the domain name while searching for her website, and the registrant would receive money to help defray the cost of operating a website.

[120] *See, e.g.*, Intermatic Inc. v. Toeppen, 947 F. Supp. 1227, 1234-36 (N.D. Ill. 1996) (holding that there are questions of fact relevant to Intermatic's unfair competition claim).

[121] For instance, nearly half the states have adopted the Model Penal Code's definition of extortion. *See* MODEL PENAL CODE § 223.4 cmt. 2(k) (1980) "A person is guilty of theft if he purposely obtains property of another by threatening to: . . . (7) inflict any other harm which would not benefit the actor." *Id.* § 223.4(7). This definition of blackmail is central case blackmail.

[122] *See generally* Kevin M. Clermont & Theodore Eisenberg, *Exorcising the Evil of Forum-Shopping*, 80 CORNELL L. REV. 1507, 1507-08 (1995) (discussing that all litigation entails forum-shopping and that this may be the determinative factor to the outcome of many trials).

[123] *See, e.g.*, Weber v. Jolly, 977 F. Supp. 327, 333 (D.N.J. 1997). Internet personal jurisdiction decisions generally take one of the following three positions: (1) a state may exercise personal jurisdiction over a defendant who "'enters[s] into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet,'"; (2) a state may exercise personal jurisdiction over a defendant where there is significant commercial interactivity and exchanges of information between the website and a host computer in the state; and 3) a state may not exercise personal jurisdiction over a defendant who maintains a "passive" website in that state (*i.e.*, the site "merely provides information or advertisements to users"). *Id.* at 333 (quoting Zippo Mfg. Co. v. Zippo Dot Com, Inc. 952 F. Supp. 1119, 1124 (W.D. Pa. 1996)).

[124] Most commentators agree that criminalizing blackmail is proper. *See, e.g.*, Murphy, *supra* note 77, at 163 (arguing that blackmail may provide "a reasonable basis for criminalization" because it is immoral and economically wasteful).

[125] Deterrence is characterized as prospective justice while retribution is characterized as retrospective justice. *See* Fletcher, *supra* note 67, at 1629. A detailed explanation of the theories underlying criminal punishment is beyond the scope of this article.

[126] Generally, criminal punishment of an action will deter others from pursuing that action, especially where the action can be effectively policed.

[127] Because cybersquatters can cause consumer confusion and increase consumer search costs, cybersquatting may be viewed as more of a crime against society than against any individual trademark owner.

[128] *See* Lanham Act, 15 U.S.C. § 1125(a)(1) (1994) (limiting trademark infringement suits to civil remedies).

[129] *See, e.g.*, Intermatic Inc. v. Toeppen, 947 F. Supp. 1227, 1233 (N.D. Ill. 1996) ("Toeppen is what is commonly referred to as a cyber-squatter.").

[130] *See, e.g.*, Henry H. Perritt, Jr., *Tort Liability, the First Amendment, and Equal Access to Electronic Networks*, 5 HARV. J.L. & TECH. 65, 119-21 (1992) ("[B]oth senders and receivers of digital electronic communication enjoy First Amendment protections, although not all regulation of persons handling information violates the First Amendment.").

[131] The Supreme Court has addressed some First Amendment issues concerning obscenity and the Internet. *See generally* Reno v. ACLU, 521 U.S. 844, 864-85 (1997) (challenging provisions of the Communications Decency Act are facially overbroad and thus violate the First Amendment).