2006

Cybertrespass and Trespass to Documents

Kevin Emerson Collins
Indiana University School of Law

CYBERTRESPASS AND TRESPASS TO DOCUMENTS

KEVIN EMERSON COLLINS*

I. INTRODUCTION

Perhaps not surprisingly, in light of the common perception that all that is valuable should be protected by property,[1] the rise of cybertrespass followed quickly on the heels of the rise of cyberspace itself, or at least its commercially profitable incarnation.

Cybertrespass arises from an understanding of the Internet in which tangible property is the central organizing principle. In its real-world, tangible manifestation, the Internet is simply a bunch of privately owned servers glued together by wires, transmission-directing boxes, and common communication protocols.[2] It is a

*Associate Professor of Law, Indiana University School of Law—Bloomington. I want to express my immense gratitude to Peggy Radin and Tom Grey for their helpful comments on various drafts of this article.

[1] *See, e.g.*, Mark A. Lemley, *Ex Ante Versus Ex Post Justifications for Intellectual Property*, 71 U. CHI. L. REV. 129, 131 & n.7 (2004).

[2] "Servers" are the computers that provide, via the Internet, a particular information resource to "clients," the computers that use the resource. *See* HARLEY HAHN & RICK STOUT, THE INTERNET COMPLETE REFERENCE 13-14 (1994). The server/client (or server/served) dichotomy may refer to either the hardware or the software performing these functions, *see id.*, but this paper uses it exclusively to refer to hardware. *But cf.* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd., 380 F.3d 1154, 1158 (9th Cir. 2004) (describing peer-to-peer file sharing software that challenges the strict server-client hierarchy and that transforms traditional client machines into limited-purpose servers).

computer network riddled with boundaries between distinct chattels with distinct owners, and it is thus riddled with boundaries between distinct private-property enclaves. Focusing exclusively on this conceptual framework of the Internet as a group of networked boxes, the advocates of cybertrespass translate to the Internet the straightforward and now familiar stories that are commonly used to justify the exclusive rights in tangible resources. Packets of information sent over the network are described as trespassory "invasions" to a server-as-chattel (unless authorized). The Internet users sending those packets come to be viewed as yet another set of cattle herders prone to externalizing the congestion costs generated by overgrazing a rival resource.[3] A legal regime that extends private control of the tangible infrastructure of the Internet to afford private control over the transmission of, access to and use of information on the Internet becomes a tool to make a server marginally more valuable to the server owner and thus to increase the server owner's incentives to provide and maintain the server.

The problem with these stories, however, is precisely the problem that Peggy Radin raises in her contribution to this symposium: They frame the issue in an unadulterated discourse of property. Cybertrespass opens the door to the propertization of information without requiring judges to consider or even acknowledge the policy benefits of free-flowing information that animate the free-speech jurisprudence of the First Amendment and the competition-enhancing public domain of intellectual property law. The invasions at issue are nothing more than information inscribed in a real-world medium—the only state in which information can exist outside of our minds and the state in which it must exist for communication to occur. Cybertrespass borrows the real-space regime that governs uses that interfere with an owner's possessory interest in a tangible chattel—You cannot take my server and use it as a doorstop—and extends it wholesale to govern the flow of inscribed information—You cannot use my server to send that particular message, and you cannot use my server to access information if you use the information in that particular manner. Cybertrespass structures new-world information policy debates—Who can access, transmit and use information on the Internet and under what circumstances can he or she do so?—around classic, old-world questions of tangible property that in isolation are ill suited to providing thoughtful answers in information-centered disputes.

In this essay, I offer only a small contribution to the ongoing cybertrespass debate that I believe allows the debate to be seen from a different perspective.[4] In

[3] *See* Garret Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1244 (Dec. 13, 1968) (introducing the term "tragedy of the commons" in the context of cattle grazing in an open field). *But see infra* note 46 (arguing that congestion costs are not true externalities even if the server owner's right to exclude is tempered by a harm requirement).

[4] The academic literature on cybertrespass is extensive. For a small sampling, see Dan L. Burk, *The Trouble With Trespass*, 3 J. SMALL & EMERGING BUS. L. 1, 29-30 (1999); Richard Epstein, *Cybertrespass*, 70 U. CHI. L. REV. 73, 82-84 (2003) (arguing that websites are more like real property than chattels); Maureen A. O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 BERKELEY TECH. L.J. 561 (2001) (arguing that web-based information aggregators are unlikely to be liable under the misappropriation doctrine); Maureen A. O'Rourke, *Shaping Competition on the Internet: Who Owns Product and Pricing Information?*, 53 VAND. L. REV. 1965 (2000).

other words, I add a new story to the mix.[5] I explore what I call *trespass to documents.* The cases applying trespass to documents are real-space, pre-Internet variants of a subset of the cybertrespass cases. They demonstrate that property rights in the tangible medium on which information is inscribed have not historically been broad enough to trump the complicated balancing of interests that characterizes information law when free-speech and competition-policy concerns are implicated. They suggest that in the past the courts have not answered questions addressing control over the flow of inscribed information by examining only the cost- and benefit-internalization rationales that lie at the heart of an economic understanding of property. They illustrate that trespass-oriented theories have been dismissed when the owner of a tangible resource seeks to use a right to exclude to obtain control over how information inscribed on that resource is used by others.

In Section II, I briefly outline the information-policy concerns that are at stake in the cybertrespass cases. I divide cybertrespass into two case-types. Distribution cases involve an Internet user who sends email through an email server en route to its final destination and a server owner who seeks to enjoin the email speech based on its content. Extraction cases involve an Internet user who accesses publicly available information on a website and a server owner who seeks to enjoin the user's continued access to the website because the user employs the information gleaned from the website in a manner that is legal yet contrary to the server owner's interests. In both case-types, a strong cause of action in cybertrespass can override the public privileges guarded by the free-speech and public-domain principles that traditionally govern the transmission and use of information.

In Section III, I review the evolution of trespass-to-chattels into cybertrespass. In its common-law formulation, trespass to chattels required a chattel owner to demonstrate actual harm to a chattel to prove an actionable trespass, but this limitation on the scope of tangible property has had a mixed reception in the cybertrespass courts when countered with the property-maximizing narratives discussed above. Broadly speaking, the courts have at times interpreted the harm requirement as a limitation on a server owner's property interest in the distribution cases but have more frequently treated it as a mere formality in the extraction cases. They have proven willing to accept that the benefits of speech and widely available information that drive First Amendment doctrine may under certain circumstances outweigh the benefits of increased cost and benefit internalization, but they have not reached this conclusion when the relevant policy concerns have involved protecting the public's right to use information that resides in public domain. In the extraction case-type, cybertrespass and property discourse have preempted (in a pragmatic, if not legal, sense) the limitations on private control over publicly available information inherent in intellectual property law.

In Section IV, I introduce the trespass-to-documents cases, including the Second Circuit opinion in *Harper & Row, Publishers, Inc. v. Nation Enterprises.*[6] These cases provide a pre-Internet extraction scenario involving document owners and document users rather than server owners and server users. Party A owns a

[5] *Cf.* Carol M. Rose, *Property as Storytelling: Perspectives from Game Theory, Narrative Theory, Feminist Theory*, 2 YALE J.L. & HUMAN. 37, 38-39 (1990) (arguing that narrative figures prominently in property rights debates).

[6] 723 F.2d 195 (2d Cir. 1983).

document, party B obtains and uses/publishes information from that document, and party A sues party B alleging trespass to the tangible document. Paralleling cybertrespass cases, the courts invoke trespass to chattels and its harm requirement as the appropriate legal framework to determine the respective rights of the parties. Unlike in the cybertrespass extraction cases, however, the courts interpret the harm requirement in a robust fashion and limit the document owner's infrastructure-based property interest.

In Section V, I explore the lessons for cybertrespass that can be drawn from the trespass to document cases. I suggest that trespass to documents is most useful as a reminder that property law has historically been tailored to prevent property rights in the media on which information is inscribed from trumping the balance of public and private rights that animates intellectual property. Despite its adoption of the old-world rhetoric of trespass, a cause of action in cybertrespass that is broad enough to allow a server owner to control information merely because the information is inscribed on an owned and tangible medium involves a radical shift from the baseline that establishes the rights of infrastructure owners and information users in real space.

II. THE CYBERTRESPASS CASE-TYPES

All cybertrespass cases involve server owners who view incoming packets of information as invasions and invoke their property interests in their tangible computers to prevent such invasions. Nonetheless, cybertrespass is not monolithic. There are two distinct cybertrespass causes of action. Each involves different software technology; each implicates the flow of information in a different direction in the server-client pairing; each implicates different policy concerns that counterbalance the cost- and benefit-internalization rationales of greater propertization. Each should be analyzed independently.

A. Distribution

I term the first case-type the *distribution* case-type because it arises when an Internet user distributes information from his own computer to other computers over the Internet through a "push" technology such as email.

Between the sender's and the recipient's machines, email is typically stored on and relayed by specialized email servers that do not belong to either party to the speech act. Each email user has a contractual account or some other relationship with one of these server owners. The server-owner plaintiffs in the distribution cybertrespass cases are therefore intermediaries.

In the distribution cases, the owners of email servers do not object to email invasions generally. In fact, the opposite is true. They expressly hold out their servers to store and direct email from and to the Internet-using public at large as a service for their account holders. The server owners object only to a limited set of email invasions based on the content of the email speech. (More precisely, the server owner discriminates against particular speakers because those speakers have in the past demonstrated that they send emails with certain messages.) In some cases, the server owner deems the speech to be low value, commercial speech; in other cases, the server owner believes that the content of the speech is harmful to its reputation.

In the distribution cases, the breadth of the property right vindicated by cybertrespass determines whether the content of email speech can be controlled by server owners or whether the information-oriented policy concerns animating First Amendment free speech jurisprudence have a role to play in shaping email speech.

B. Extraction

I call the second case-type the *extraction* case-type because it involves email users who seek to extract or download information from a server that hosts a publicly accessible web page. "Pull" technologies such as the World Wide Web transmit information to an Internet user only after the Internet user has sent a request for that information. In the extraction cases, the server owner seeks to exclude this incoming, "dumb" request for information, not the outgoing "smart" and information-laden signal that distributes a web page to an Internet user.

As in the distribution cases, server owners in the extraction cases do not object to Internet users in general downloading information from their servers. Website owners usually desire and often actively pay to increase this diffusion of the posted information. Nor do the extraction cases involve contracts or technological protection measures. The website is made available to the public at large, and the public is invited to send requests for the posted information to the web server. The server owners object only to particular individuals' extraction of information from their servers because those individuals use the downloaded information in a manner that is detrimental to the server owners' interests. To date, the extraction cases have involved Internet users who have downloaded information from business websites and then engaged in a competing enterprise,[7] but there is nothing preventing a website owner from bringing a cybertrespass cause of action to prevent further expressive harm if the Internet user criticizes the website or engages in counter speech.

Because the server owner may exclude Internet users who are using factual information in a manner that is condoned, or even encouraged, under competition policy laws or who are transforming expressive material in a manner that is permitted by copyright, the scope of property in networked servers in these cases determines the extent to which the policy concerns animating the public domain of intellectual property law structure how the public may use information made available via the World Wide Web.

III. FROM TRESPASS-TO-CHATTELS TO CYBERTRESPASS

Regardless of whether a case involved distribution or extraction, cybertrespass arguments in the courts have had a common format. Courts have accepted the server owners' arguments that the flow of information on the Internet presents a new riff on trespass and that property interests in the tangible computers present relevant considerations in determining who can control transmission of and access to information. The debate has not addressed the existence of a server owner's property interest but has rather queried the appropriate scope of that interest. How broad is the individual server owner's possessory interest vis-a-vis the processor and the memory-consuming electronic signals sent by Internet users over the network to the server-as-tangible-object? What rights to exclude does that server owner possess to vindicate this interest, and what privileges of access are vested in the Internet-

[7] *See infra* Section III.C.2.b (discussing the extraction cases).

using public? Courts have in turn sought to answer these questions with resort to the doctrine of trespass to chattels.[8] The server box is, after all, a chattel.[9]

Ironically, trespass to chattels was used as a tort to vindicate property interests in communication networks decades before the advent of the Internet: Errant digging that severed or damaged buried cables commonly supported actions in trespass to the cable.[10] The trespass to chattels doctrine had to evolve in three ways, however, before a server owner could call upon it to vindicate a possessory interest sufficiently broad to exclude an information-transmitting signal from a networked server.

First, trespass—whether to land or to chattels—traditionally recognized only tangible invasions as actionable invasions. Shovels are clearly tangible, but jostling electrons are not. The tangibility requirement therefore had to evolve before courts could label interfering electronic signals as actionable interferences.

Second, the courts had to reconcile a private right to exclude with the publicly accessible nature of an Internet server. Cables are buried to avoid physical tampering, implying that a cable owner intends to reserve his right to exclude shovels, whereas servers are voluntarily networked to each other and to the computers of Internet users, suggesting that perhaps the general public has an enduring interest in the servers as long as the servers remain connected to the network.

Third, the courts had to interpret the harm requirement that traditionally limited the scope of the chattel owner's possessory interest. Severing a cable damages the cable-as-chattel, but does sending the type of coded instructions a server was designed to process harm the server-as-chattel?

In this section, I trace and analyze each of these evolutionary steps, but I place particular emphasis on the third step. The harm requirement has proven to be the most contested aspect of the cybertrespass cause of action, and it is the question on which trespass to documents may shed the most light.

A. *Intangibility*

In *Thrifty-Tel, Inc. v. Bezenek*,[11] a California appeals court upheld a cause of action in trespass to a remote computer system unrelated to the Internet. The plaintiff and computer owner Thrifty-Tel provided a long-distance telephone service. Subscribers received both an access code (a telephone number used to dial into the Thrifty-Tel computer system) and an authorization code. The defendants were

[8] Casting servers as the virtual property of cyberspace, some server owners have argued that trespass to land is the most appropriate legal doctrine on which to model cybertrespass. *See, e.g.*, Epstein, *supra* note 4, at 82-84 (arguing that websites are more like real property than chattels). These arguments, however, have been most effective in the courts as arguments suggesting that the harm requirement in trespass to chattels should be an easily satisfied formality. *See infra* Section III.C (discussing robust and formalistic interpretations of the harm requirement in trespass to servers).

[9] "Movable or transferable property; personal property; esp., a physical object capable of manual delivery and not the subject matter of real property." BLACK'S LAW DICTIONARY (8th ed. 2004).

[10] W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 14, at 86-87 (5th ed. 1984) [hereinafter PROSSER & KEETON].

[11] 54 Cal. Rptr. 2d 468, 471 (Cal. Ct. App. 1996).

children who, using their parent's access codes, set up an automated dialing process to serially query the Thrifty-Tel system with computer-generated numbers—a brute force, trial and error attempt to discover a working authorization code.[12] Thrifty-Tel brought suit for damages, and the appeals court held that the electronic impulses conveying the children's calls were trespassory invasions to Thrifty-Tel's computer-system chattel.[13]

The discussion of the plaintiff's property-related claims in the *Thrifty-Tel* opinion raises concerns about intangibility in two guises. In the trial court, Thrifty-Tel brought and prevailed on only one property claim—a conversion claim alleging that the defendants effectively stole information in the form of a confidential access phone number that had been issued by Thrifty-Tel only to their parents. The appeals court refused to affirm on this conversion claim, however, reasoning that theft of an intangible good, such as information, likely could support a conversion claim.[14] Furthermore, even if a state law claim for conversion of intangible information did exist, it would likely be preempted by federal copyright law,[15] and copyright law would not provide a remedy because information policy concerns prevent copyright from reaching the unauthorized copying of factual information such as a single access number.[16] Instead, to accomplish the same end and to support the verdict below, the appeals court substituted the trespass claim for the information-conversion claim.[17] Here, the second concern about intangibility arises, this time a concern about the relative intangibility of the invading electronic signals as trespass to chattels was not available at common law to vindicate interferences with personal property that were not considered "physical."[18] But this time the intangibility concern proved surmountable. Borrowing from the more developed doctrine of trespass to land, the *Thrifty-Tel* court relied on cases holding that small particles, traditionally deemed intangible, could support actionable invasions to land,[19] and

[12] *Id.* (noting that defendants generated over 1300 calls during seven hours).

[13] *Id.* at 472-73.

[14] *Id.* at 472 & n.5 (noting that courts have "refused to recognize as conversion the unauthorized taking of intangible interests that are not merged with, or reflected in, something tangible").

[15] Statutory copyright preemption bars state law causes of action if they protect rights "equivalent" to those protected by § 106, and the work they protect is both fixed in a tangible medium of expression and within the "subject matter of copyright." 17 U.S.C. § 301(a) (2006).

[16] *See, e.g.*, Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 344 (1992) ("[F]acts are not copyrightable."); *id.* at 349-50 (discussing how the fact/expression dichotomy works to promote "the progress of science and art").

[17] *Thrifty-Tel*, 54 Cal. Rptr. 2d at 472-73.

[18] RESTATEMENT (SECOND) OF TORTS § 217 cmt. e (1965) ("'Intermeddling' means . . . physical contact with the chattel."); *cf.* § 218 cmt. h (noting that "[i]n the great majority of cases" value to the possessor is impaired "only by some impairment of the physical condition of the chattel").

[19] *Thrifty-Tel*, 54 Cal. Rptr. 2d at 473 n.6. *Martin v. Reynolds Metals Co.* was one of the first modern cases to discard the intangibility of an invasion as a per se bar to trespass to land.

thus paved the road for Internet data packets to be labeled actionable invasions in later cybertrespass cases.[20]

The role of intangibility in *Thrifty-Tel* is critical to understanding cybertrespass. *Thrifty-Tel* relied on an action in trespass to a computer system when the action based on property rights in intangible information failed to provide a remedy. With this substitution, the court elided two distinct concerns. Thrifty-Tel initially sought to vindicate a property interest in its truly intangible *information* resource, but when the relevant information-based right proved non-existent, the court slipped in an injunction based on the unauthorized invasion of the computer-system *infrastructure* by the semi-tangible inscription of information required for the infrastructure to convey the information. Thus, from its first step, the evolution of cybertrespass has been affected by the ability of cybertrespass to permit a private party to control uses of information that a well-formulated information policy might place beyond that party's control.

B. Network-by-Consent

The servers at issue in the cybertrespass cases constitute a public network in the sense that the processing capacity of a server is by default equally accessible by all Internet users. Server owners connect their processing capacity to the Internet, minimize software barriers deterring use by the general Internet-using public,[21] and

342 P.2d 790, 793-94 (Or. 1960) (*en banc*) (describing the intangibiliy bar as a doctrinal appendix that the law has needlessly carried forward from less-informed times).

[20] The indirect reliance of cybertrespass courts on the trespass to land cases by way of the *Thrifty-Tel* analysis is ironic. *See supra* note 19. The trespass to land cases eliminating the intangibility bar, including those in California, created a harm requirement to replace it, whereas the cybertrespass courts were in the process of reducing the harm requirement from trespass to chattels to a mere formality when they eliminated the intangibility bar. *See* San Diego Gas & Elec. Co. v. Superior Court, 920 P.2d 669, 695-96 (Cal. 1996) (holding that only intangible invasions that cause physical damage to land are actionable trespasses); *see also* Mock v. Potlach Corp., 786 F. Supp. 1545, 1550-51 (D. Idaho 1992) ("[I]f the intangible invasion causes *substantial damage* to the plaintiff's property, this damage will be considered to be an infringement on the plaintiff's right to exclusive possession."); Maddy v. Vulcan Materials Co., 737 F. Supp. 1528, 1539 (D. Kan. 1990) ("The plaintiff claiming trespass must prove that the intangible invasion resulted in substantial damages to the plaintiff's land."); Borland v. Sanders Lead Co., 369 So.2d 523, 529 (Ala. 1979) (requiring a plaintiff who sought damages based on airborne particles to demonstrate "substantial damages to the Res" to recover in trespass); Wilson v. Interlake Steel Co., 649 P.2d 922, 924 (Cal. 1982) ("Noise alone, without damage to the property, will not support a tort action for trespass."); Pub. Serv. Co. of Colorado v. Van Wyk, 27 P.3d 377, 389-91 (Colo. 2001) ("An intangible intrusion onto property cannot result in a trespass unless the intrusion causes physical damage to the property."); Williams v. Oeder, 659 N.E.2d 379, 383 (Ohio App. 1995) (permitting an action in trespass for airborne dirt only if the invasion causes substantial damage); Bradley v. Am. Smelting and Refining Co., 709 P.2d 782, 790 (Wash. 1985) (adopting the *Borland* rule). *But see* Stevenson v. E.I. DuPont de Nemours and Co., 327 F.3d 400, 405-06 (5th Cir. 2003) (interpreting Texas law not to limit trespass to "direct and tangible" invasions but holding that no showing of substantial damage to property was required, although damage to livestock on the land had been shown).

[21] In the cybertrespass cases, the electronic signals do not bypass any software-enabled technological devices that are intended by the server owners either to prevent the incoming

expend resources to encourage users to visit, as a larger user base translates into a larger personal gain. The property question presented by cybertrespass is specific to networked servers: Assuming a right to exclude from an isolated server,[22] does the voluntary contribution of one's server to a public and otherwise unavailable collective resource affect the property interests in the server that existed prior to its participation in the network?

In *CompuServe Inc. v. Cyber Promotions, Inc.*,[23] a federal district court answered this question in the negative and outlined the principle of network-by-consent. In *CompuServe*, the defendant's business model was predicated on sending unsolicited commercial email, and CompuServe, a commercial provider of Internet access and email accounts, brought suit to enjoin defendants from sending this bulk email to its servers, a necessary point of transit for messages sent to CompuServe customers. Although the court accepted that CompuServe's business-oriented decision to make its server a part of the Internet network was a "tacit invitation" that held open the server to the public and gave would-be trespassers a privilege to send email to the server,[24] it also concluded that any such implicit general invitation could be, and had in fact been in this case, rescinded by a specific revocation.[25] Under a network-by-consent model, property rights in an aggregated resource are no more and no less than the sum of the property rights in the individual units of the resource. Units of the networked resource are legally linked only by a revocable invitation of each property owner to access each separately proprietized unit.

The California Supreme Court expressed the opposite viewpoint in *Intel Corp. v. Hamidi*—that the networking of servers in a publicly accessible fashion involves an alteration of property rights beyond the granting of revocable licenses.[26] In *Intel*, the court characterized the server owner's decision to connect its server to the Internet as

signals from flowing onto the server or to protect information resident on the server from being copied. Technologically, the servers are open to the public for the uses at issue.

[22] Whether or not such a property right exists at common law is addressed *infra* in Section III. C.

[23] 962 F. Supp. 1015 (S.D. Ohio 1997).

[24] *Id.* at 1023-24.

[25] *Id.* at 1024 (finding consent rescinded by cease and desist letters). Another cybertrespass court has extended the network-by-consent reasoning to suggest that a specific revocation is not necessary: The scope of the original implied consent granted to the public can be construed as a majoritarian default term in an implied contract and thus as limited to those practices that a reasonable server owner would have authorized. *See* eBay v. Bidder's Edge, 100 F. Supp. 2d 1058, 1070 (N.D. Cal. 2000) ("Even if BE's web crawlers were authorized to make individual queries of eBay's system, BE's web crawlers exceeded the scope of any such consent when they began acting like robots by making repeated queries."). Such a limited scope of implied consent should, in theory, turn on the customs of Internet usage, an inquiry that the eBay court did not make. *Id.*

[26] Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003). The discussion of consent in *Intel* is dicta because the *Intel* court held that the server owner had no right to exclude harmless invasions. *See* text accompanying *infra* notes 61-63. The *CompuServe* court characterized network-by-right as an "argument that because an establishment invites the public to enter its property for business purposes, it cannot later restrict or revoke access to that property," and dismissed it. 962 F. Supp. at 1024.

one in which the server owner "necessarily contemplated . . . unsolicited as well as solicited communications from other companies and individuals," and the court thus deemed the consent granted by this decision to include "virtually inevitable" advance notice that "some communications would, because of their contents, be unwelcome."[27] Under this theory of network-by-right, the "tacit invitation" for the Internet-using public to use the server results in a public privilege of use that is not divisible into narrower, revocable privileges as to individual defendants.

Public network-by-right has support at common law as a public policy limitation on an individual landowner's right to exclude when he opens his land to public entry,[28] and has been reinforced by statute when the activity in which the public engages on the land is public in nature.[29] Nonetheless, courts have been hesitant to define property rights in a chattel in a relational manner—that is, as dependent upon their physical context—rather than as an inherent attribute of an object, so the network-as-consent model has largely prevailed. Network-by-consent is a precondition of a successful cause of action in cybertrespass, but it is not an inevitable result of applying property principles to networked servers.

[27] 71 P.3d at 308.

[28] At common law, a general invitation to the public to enter a parcel of land can limit a landowner's right to revoke consent so narrowly as to be unreasonable. Uston v. Resorts Int'l Hotel, Inc., 445 A.2d 370, 375 (N.J. 1982) ("[W]hen property owners open their premises to the general public in the pursuit of their own property interests, they have no right to exclude people unreasonably."); *id.* at 372 ("[T]he common law right to exclude is substantially limited by a competing common law right of reasonable access to public places.").

The Supreme Court addressed a similar common-law issue concerning the permissible ratio between the breadth of the default public invitation and the narrowness of an individual revocation of consent in its line of cases addressing the constitutional protection of free speech in shopping centers. In *Amalgamated Food Employees v. Logan Valley Plaza, Inc.*, the Court held:

> [Because the shopping center] 'is freely accessible [architecturally] and open [by invitation] to the people in the area and those passing through,' the State may not delegate the power, through the use of its trespass laws, wholly to exclude those members of the public wishing to exercise their First Amendment rights on the premises in a manner and for a purpose generally consonant with the use to which the property is actually put.

391 U.S. 308, 318-319 (1968) (quoting Marsh v. Alabama, 326 U.S. 501, 508 (1946)). In other words, as in *Intel*, the broad invitation issued to the public to use the property, coupled with the property's physical accessibility from public space, was irrevocable insofar as the landowner sought to exclude specific individuals using the property within the scope of the initial invitation. Subsequently, however, the Court rejected this principle of a First Amendment irrevocable license in *Lloyd Corp. v. Tanner*, labeling it "an attenuated doctrine of dedication of private property to public use" and stating that "property [does not] lose its private character merely because the public is generally invited to use it for designated purposes." 407 U.S. 551, 569 (1972). *Cf.* Hudgens v. Nat'l Labor Relations Bd., 424 U.S. 507, 521 (1976) (interpreting *Lloyd Corp.* as a case that did not involve state action).

[29] *See, e.g.*, Minn. Stat. §§363A.11 (2005) (Minnesota Human Rights Act public accommodation statute).

C. The Harm Requirement

Consent to use a resource, however, is irrelevant if the resource owner lacks the property right to exclude the particular use at issue. Internet users' most common argument in cybertrespass cases has been that server owners have no right to exclude because they cannot demonstrate harm to the server.[30] The remainder of this section outlines the harm requirement in trespass to chattels as it existed at common law and as it has been applied in cybertrespass.

1. Trespass to Chattels

Although conversion and trespass to chattels are both torts that grant the possessors of a tangible personal good a right to exclude in real space, it has fallen to trespass to chattels—the broader, yet less valuable and thus less used, legal backstop to conversion in real space[31]—to provide the doctrinal source material from which to craft trespass to servers in cyberspace. Conversion requires a showing of harm to the chattel owner's interest in possession of the chattel,[32] an interest not challenged in the cybertrespass cases, whereas trespass to chattels requires only a weaker showing of harm. One of the enduring questions in the doctrinal cybertrespass debate is historically how much weaker it has been.

The historical exclusion of harmless or *de minimus* interferences from the scope of trespass to chattels is summarized in two telescoping provisions in §§ 217 and 218

[30] The existence of an affirmative-defense privilege is another such argument. *See generally* PROSSER & KEETON, *supra* note 10, § 16, at 109 (noting that a privilege exists where "the defendant has acted to further an interest of such social importance that it is entitled to protection, even at the expense of damage to the plaintiff," or where "current ideas of what will most effectively promote the general welfare" suggest the defendant's conduct should be permitted). Because trespass to land is the most developed of the trespass doctrines, its privileges have been used as a model for unsuccessful arguments that a privilege to cybertrespass should protect Internet users who access a server. *See, e.g.*, CompuServe Inc., v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1025 (S.D. Ohio 1997) (holding that CompuServe is not a public utility under Ohio law). The existing affirmative-defense privileges have proven inapplicable because trespass to land carries a presumption that the privileges should be narrowly construed. PROSSER & KEETON, *supra* note 10. There is no common-law privilege addressing the right to enter land for the purpose of gathering or disseminating information. *But see* Curtis J. Berger, Pruneyard *Revisited: Political Activity of Private Lands*, 66 N.Y.U. L. REV. 633, 661-670 (1991) (suggesting that state courts should create a "Common-Law 'Public Forum'" permitting speakers to enter land for the purpose of engaging in speech).

[31] *See* PROSSER & KEETON, *supra* note 10, § 13, at 85-86 (stating that the "chief importance" of trespass to chattels "now is . . . for interferences with the possession of chattels which are not sufficiently important to be classed as conversion . . . . Trespass to chattels survives today, in other words, largely as a little brother of conversion."). Conversion is used more frequently to seek redress for interference with real-space chattels because its remedy is stronger. *Compare* Zaslow v. Kroenert, 29 Cal. 2d 541, 551 (1946) (noting that trespass-to-chattels damages are "the actual damages suffered by reason of the impairment of the property or the loss of its use"), *with* PROSSER & KEETON, *supra* note 10, §14, at 87 (noting that damages for conversion "compel the defendant to pay the full value of the thing with which he has interfered").

[32] RESTATEMENT (SECOND) OF TORTS, *supra* note 18, § 222A(1) (1965).

of the Second Restatement of Torts. While § 217 describes the tort as applying broadly to any intentional "using or intermeddling with a chattel,"[33] § 218 delimits the narrower range of conduct that is "actionable" because it interferes with the chattel owner's "legally protected interest."[34] Relevant to cybertrespass, § 218 states that liability for trespass to a chattel exists "if, but only if . . . (b) the chattel is impaired as to its condition, quality, or value, or (c) the possessor is deprived of the use of the chattel for a substantial time."[35] Thus, § 218 vests the public with the entitlement to engage in "harmless" interferences with the chattel.[36] The Restatement emphasizes the existence of a harm requirement when it distinguishes the chattel owner's interest in possession from the landowner's interest in exclusive possession:

> The interest of the possessor of a chattel in its inviolability, unlike the similar interest of a possessor of land, is not given legal protection by an action for nominal damages for harmless intermeddlings with the chattel. In order that an actor who interferes with another's chattel may be liable, his conduct must affect some other and more important interest of the possessor.[37]

The Restatement offers two cases illustrating that, although relatively infrequent, inactionable intermeddling is not a null set in real space. A child does not commit a trespass to chattel when she encounters a dog on the porch of a neighborhood candy store and "climb[s] on his back and pull[s] his ears."[38] While the condition, quality, or value of the dog was obviously transitorily impaired for the duration of the ear

[33] *Id.* § 217.

[34] *Id.* cmt. a (establishing that a trespassory act that meets the requirements of § 217 but of § 218 is not "actionable because it does no harm to the chattel or to any other legally protected interest of the possessor"). Section 217 "does not purport to state the circumstances or conditions under which a trespass makes the actor liable. These are set forth in [§ 218]." *Id.*

[35] *Id.* § 218.

[36] A minority of commentators suggests that no harm requirement exists in a trespass to chattels cause of action that seeks only an injunction and does not request even nominal damages. *See* Intel Corp. v. Hamidi, 114 Cal. Rptr. 2d 244, 249 (Cal. Ct. App. 2001) ("A trespass to chattels is actionable *per se* without any proof of actual damage. Any unauthorized touching or moving of a chattel is actionable at the suit of the possessor of it, even though no harm ensues." (quoting SALMOND ON TORTS § 6.2, at 95 (21st ed. 1996))); Intel Corp. v. Hamidi, 71 P.3d 296, 318-21 (Cal. 2004) (Brown, J., dissenting) ("[N]umerous cases have authorized injunctive relief to safeguard the inviolability of personal property."); Epstein, *supra* note 4, at 77-78 & n.13 (discussing the English rule).

[37] RESTATEMENT (SECOND) OF TORTS, *supra* note 18, § 218 cmt. e (1965). This distinction between trespass to land and trespass to chattels reverberates through the tort-law hornbooks. *See, e.g.*, FOWLER V. HARPER, FLEMMING JAMES & OSCAR S. GRAY, THE LAW OF TORTS §2.15 (3d ed. 1996) [hereinafter HARPER & JAMES] ("Unlike trespass to land, under trespass to chattels no action could be maintained for a mere harmless intermeddling with goods. The possessor's proprietary interest in the inviolability of his personal property did not receive the protection that the similar interest in the possession of land or the dignitary interest in the inviolability of the person receives.").

[38] Glidden v. Szybiak, 63 A.2d 233, 233 (N.H. 1949).

pulling, "[n]o claim was advanced at the trial that the dog . . . was in any way injured . . . . Consequently [the child] could not be held liable for a trespass to the dog."[39] Similarly, a two minute search of a truck in which "[n]either the truck nor its contents were damaged in any manner" did not impair the condition of the truck under § 218(b) and was not a deprivation of use "for a substantial time" under § 218(c).[40] Nor does the harm requirement of § 218 sap the broader § 217 of all legal significance: Technical but inactionable trespasses under § 217 provide the chattel owner with a defense to a potential battery claim brought by the trespasser because the owner has an affirmative-defense privilege to use reasonable force to protect the chattel.[41]

2. Cybertrespass

Given that trespass to chattels is the tort from which cybertrespass descends,[42] what should constitute actionable harm in the cybertrespass cases?[43] The array of possible harm requirements in the cybertrespass cases is best understood through two paired and nested categories.

The initial distinction is between "information harm" and "rival harm." Information harm is injury to the server owner resulting from the content of the information conveyed or the use to which the recipient of a transmission puts the content after the transmission has occurred. In contrast, rival harm flows from the fact that the server's processing capacity is a rival resource in which one person's use of a portion of the resource makes that portion unavailable for simultaneous use by another person.[44] Rival harm is indifferent to the content of the information

[39] *Id.* at 235.

[40] Koepnick v. Sears Roebuck & Co., 762 P.2d 609, 619 (Ariz. Ct. App. 1998). An actionable deprivation of use "must be for a time so substantial that it is possible to estimate the loss caused thereby." RESTATEMENT (SECOND) OF TORTS, *supra* note 18, § 218(c) cmt. i (1965).

[41] *Id.* § 217 cmt. a ("[T]he fact that one person is committing a trespass to another's chattel [under § 217], while it may not be actionable because it does no harm to the chattel . . . affords the possessor a privilege to use force to defend his interest in its exclusive possession."); *id.* § 218 cmt. e ("Sufficient legal protection of the possessor's interest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference.").

[42] *But see supra* note 8 (noting that some advocates of strong server-based property rights propose trespass to land as the correct doctrinal model).

[43] The question of actionable harm in the cybertrespass cases is a narrow one. The cybertrespass cases pertain only to invading electronic signals sent over a network connection, not to baseball bats. Furthermore, they address only a limited range of possible "invading" signals: they involve Internet users who seek to obtain from the server the technological service that the server's software is designed to provide; they do not address whether property in networked servers encompasses the right to exclude signals that exercise technological might to reprogram the server. In other words, for the purpose of the cybertrespass cases, they take the software-programmed server as the relevant tangible resource to which property rights are applied.

[44] Because the cybertrespass cases address only incoming electronic signals that are technologically the type of signals any particular server and its software were intended to

encoded by the invading signals and is incurred by the act of transmitting or storing the signals.[45]

Within the category of rival harm, the second distinction is between actual and potential rival harm. Actual rival harm results when one Internet user's signals impose short-term congestion costs on the server owner or on other Internet users accessing the server, that is, when one user slows down or prevents server access by others.[46] However, not every use of a rival resource will impose congestion costs on other users: Often there is enough of the resource relative to the intensity of usage that one person's use of the resource does not measurably affect another person's use. At the moment that the resource is used, such an abundant rival resource is plenteous.[47] However, even with a momentarily plenteous resource, there is the potential for rival harm to occur whenever a resource is used because there is always the possibility of a sudden increase in usage that might render the previously plenteous resource scarce. Potential rival harm thus results from any use of a server because one user's consumption of server resources in theory would prevent another user from consuming those resources if that other user were to attempt to do so.

process, *see supra* note 43, the only possible type of harm to the server as a tangible chattel is harm resulting from rivalrous consumption and congestion costs, *see infra* note 46.

[45] Advocates of limited property regimes in cyberspace often elide these distinct infrastructure and information concerns. *See, e.g.*, Epstein, *supra* note 4, at 83 (eliding the movable nature of the tangible server and the costs involved in changing domain names); Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439 (2003). *But see* Carol M. Rose, *Romans, Roads, and Romantic Creators: Traditions of Public Property in the Information Age*, 66 LAW & CONTEMP. PROBS. 89, 90 (distinguishing between "Intellectual Space" and "Tangible Space").

[46] *Cf.* RICHARD POSNER, ECONOMIC ANALYSIS OF LAW 37 (5th ed. 1998) (discussing the costs imposed on all farmers by an individual farmer's decision to pasture more cows in a natural pasture and analogizing the situation to highway congestion). Whether these congestion costs are true externalities that would lead to market failure, however, is unclear. An externality exists only when there is a cost external to any individual actor's self-interest calculation that results in a decrease in overall social welfare, that is, when a cost is "external to market processes of decision." *Id.* at 81; S.J. Liebowitz & Stephen E. Margolis, *Network Externality: An Uncommon Tragedy*, J. ECON. PERSP., Spring 1994, at 135 (reserving the term externality for a cost due to which "the equilibrium exhibits unexploited gains from trade"). According to this definition, and not one defining an effect external to the decision-making process of an individual resource user, *cf.* Julie E. Cohen, Lochner *in Cyberspace: The New Economic Orthodoxy of "Rights Management,"* 97 MICH. L. REV. 462, 539-42 (1998) (discussing the ambiguity in the definition of "externality"), congestion costs of server use are not externalities even if a harm requirement limits a server owner's right to exclude. As soon as congestion costs are incurred, the server owner (who benefits from the public's use of the server) will internalize those costs and can exercise his right to exclude.

[47] A plenteous resource is one that is not scarce, or that is "so plentiful or so unbounded that it is not worth the effort to create a system of resource management for them, or—stated differently—things for which the difficulty of privatization outweighs the gains in careful resource management." Carol M. Rose, *The Comedy of the Commons: Custom, Commerce, and Inherently Public Property*, 53 U. CHI. L. REV. 711, 717 (1986). A resource that is plenteous in a narrow time frame may be scarce in broader time frame if there is a likelihood of the resource becoming scarce in the near future or on a cyclical basis. *Cf. infra* note 78 (discussing a harm requirement based on the likelihood of future congestion).

Cybertrespass courts have generally held rival harm to be actionable and information harm to be inactionable,[48] but they have reached a variety of conclusions on whether the harm requirement is robust, requiring a showing of actual rival harm, or whether it is weak, requiring only a showing of potential rival harm. If the former option is chosen, then server owners can control the flow of information only under particular circumstances defined independently of the content of the information at issue. If the latter option prevails and the harm requirement is satisfied by a showing of potential rival harm, harm becomes an ever-present formality and cybertrespass becomes an effective tool to vindicate information harm in practice, if not in name. Through a survey of the litigated cybertrespass cases, the following subsections explore the definitions of actionable harm that have been adopted and illustrate the marginal benefit that server owners can internalize when a weak harm requirement permits them to control information that would, under information-centric rather than infrastructure-centric laws, remain beyond their control.

a. Distribution Cases

The *CompuServe* case is a representative distribution case. Like many Internet service providers, CompuServe owns a server that is a way station for email addressed to its customers; the server relays all email between its customers and any other Internet user.[49] In its cybertrespass case, CompuServe convinced a federal district court to grant an injunction excluding a defendant who had been sending bulk commercial messages or "spam" to CompuServe's customers. Most of the distribution cases mimic *CompuServe* closely,[50] but *Intel Corp. v. Hamidi*[51] hints at the potential breadth of the case type: The quantity of email relayed by the server was relatively small,[52] the server-owner plaintiff was a corporate employer, and the defendant was a former employee of the corporation who sent messages to current employees at their business email addresses, raising legal and social issues regarding their conditions of employment. The final difference between *Intel* and *CompuServe* is the result: After lower *Intel* courts followed *CompuServe* and granted Intel an injunction,[53] the California Supreme Court vacated it.[54]

[48] Information harm cannot even trigger liability under trespass to land. *See* Wilson v. Parent, 365 P.2d 72 (Or. 1961) (concluding that neither the vile and obscene gestures nor the profane language of the plaintiff's son-in-law, who resided on adjoining property, constituted trespassory invasions). *But see* Epstein, *supra* note 4, at 81-82 (arguing that the server owner's decision to bring suit is dispositive evidence of actionable harm).

[49] The typical email account stores incoming email on a centralized server, owned by someone other than the sender or recipient, and the final recipient periodically downloads the email to his client computer. *See* Intel Corp. v. Hamidi, 71 P.3d 296, 308-09 (Cal. 2003).

[50] America Online, Inc. v. LCGM, Inc., 46 F.Supp.2d 444 (E.D. Va. 1998); America Online, Inc., v. IMS, 24 F.Supp.2d 548 (E.D. Va. 1998); Hotmail Corp. v. Van$ Money Pie Inc., No. C-98 JW PVT ENE, C 98-20064 JW, 1998 WL 388389 (N.D. Cal. Apr. 16, 1998).

[51] 71 P.3d 296 (Cal. 2003).

[52] The defendant sent six mass emails over a twenty-one month period, each directed at between 8000 and 35,000 current Intel employees. *Id.* at 301.

[53] Intel Corp. v. Hamidi, 114 Cal. Rptr. 2d 244 (Cal.App.4th 2001); Intel Corp. v. Hamidi, No. 98AS05067, 1999 WL 450944 (Cal. App. Super. Apr. 28, 1999).

None of the speech in these distribution cybertrespass cases was wrongful based only on its content: The information transmitted was not alleged to constitute false advertising, defamation or invasion of privacy.[55] The information being transmitted was thus the type of information that the policy concerns underlying the information-based torts have determined should flow in an unfettered fashion to benefit society. Nonetheless, from the server owner's perspective, the speech was undesirable and the content of email motivated the server owners to seek a legal remedy.[56] Unable to use a tort that examined the content of the transmission because such torts have been tailored to accommodate information policy concerns, the server owners—like the computer system owner in *Thrifty Tel*[57]—invoked their property rights in their tangible servers. Provided the property rights include the right to exclude any electronic impulses passing over the network, this switch of legal theories offered the server owners a big upside and very little downside. Once the cause of action sounded in tangible property, the server owners successfully argued that they could lawfully engage in content-based discrimination because the server was privately owned property, not a government-owned public forum in which First Amendment rights would have to be considered.[58] Using their property rights to control the flow of information, the server owners could craft rules of information policy based purely on their own self-interest without any consideration of the collective public interest.

Yet even after the issue was framed as one of tangible property, a potentially dispositive question remained: What type of harm is required to satisfy the harm requirement in trespass to server-as-chattel, and could the server owners allege it in a given case? On one level, the courts routinely sided with the emailing defendants. Perhaps wary of the server owners' desire to use trespass to control the flow of information, none of the courts have held that information harm alone is sufficient to satisfy the harm requirement of cybertrespass in the distribution cases. The fact that CompuServe disliked commercial speech or that the employee's speech was against Intel's self-interest was not, in itself, harm that could trigger a right to exclude. On

[54] *Intel*, 71 P.3d at 300.

[55] *See id.* (listing information-centric torts that look to the content of the information transmitted to determine liability).

[56] Internet service providers considered the commercial spam to be low-value speech; the former employee's speech undermined Intel's relationship with its employees. It is interesting to contrast these two cases on the extent to which the server owner's perspective can be seen as an accurate proxy for the end user's desires. CompuServe alleged that the defendants' messages were unwanted by its customers, CompuServe Inc., v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1023 (S.D. Ohio 1997) (discussing customer complaints and terminated accounts due to bulk email in general or the defendants' conduct in particular), whereas the defendant in *Intel* "offered to, and did, remove from his mailing list any recipient who so wished," *Intel*, 71 P.3d at 299.

[57] *See supra* Section III.A.

[58] When the courts have determined that the baseline entitlements established by the server owner's property rights include the right to exclude the email, they have routinely rejected the emailers' free speech defenses. *CompuServe*, 962 F. Supp. at 1025-27 (rejecting a First Amendment defense); *Intel*, 114 Cal. Rptr. 2d at 252-58 (rejecting free speech defenses based on both the First Amendment and the California Constitution).

another level, however, this recognition of rival . rather than information harm sometimes proved a pyrrhic victory for the defendants as the courts announced rival harm requirements spanning the spectrum from actual to potential.

One reading of *CompuServe* is that the court established an actual rival harm standard and found this standard satisfied by the large quantity of email sent by the spamming defendants.[59] Another more plausible reading, however, suggests that *CompuServe* required only a showing of potential rival harm as CompuServe never even alleged that its customers' access to the storage space or processing power was impaired. The court stated that "[t]o the extent that defendants' multitudinous electronic mailings demand the disk space and drain the processing power of plaintiff's computer equipment, those resources are not available to serve CompuServe subscribers,"[60] but the court never found that CompuServe subscribers attempted to or wanted to use those resources. Under this second reading, the court found harm based on the emailers' use of a rival-yet-plenteous good: The unavailability of the server for potential use by others suffices to trigger cybertrespass, and any use of a server is theoretically actionable.

In contrast, the highest court in *Intel* insisted that the plaintiff server owner demonstrate actual rival harm to make out a cause of action in cybertrespass and found that the facts of the case did not demonstrate any such actionable harm.[61] It expressly rejected a theory of harm based on potential rival use,[62] found that Intel's true reason for objecting to the messages was the information harm the messages caused and held that such harm was inactionable under cybertrespass.[63]

[59] *CompuServe*, 962 F. Supp. at 1019 (finding that "the volume of messages generated by [defendants'] mass mailing places a significant burden on [CompuServe's] equipment"); *cf.* Hotmail Corp. v. Van$ Money Pie Inc., No. C-98 JW PVT ENE, C 98-20064 JW, 1998 WL 388389, *7 (N.D. Cal. Apr. 16, 1998) (noting that the defendants' conduct involved "filling up Hotmail's computer storage space and threatening to damage Hotmail's ability to service its legitimate customers").

[60] 962 F. Supp.at 1022.

[61] *Intel*, 71 P.3d at 303-04 ("[T]he undisputed evidence revealed no actual or threatened damage to Intel's computer hardware or software and no interference with its ordinary and intended operation . . . . Intel presented no evidence its system was slowed or otherwise impaired by the burden of delivering Hamidi's electronic messages. Nor was there any evidence transmission of the messages imposed any marginal cost on the operation of Intel's computers.").

[62] *Id.* at 306-07 ("That [the defendant's] messages temporarily used some portion of the Intel computers' processors or storage is . . . not enough; Intel must, but does not, demonstrate some measurable loss from the use of its computer system.").

[63] *Id.* at 307-08 ("Intel's complaint is . . . about *the contents of the messages* rather than the functioning of the company's e-mail system . . . . Intel's position represents a[n] . . . extension of the trespass to chattels tort, fictionally recharacterizing the allegedly injurious effect of a communication's *contents* on recipients as an impairment to the device which transmitted the message."). To avoid a conflict with *CompuServe*, however, *Intel* inaccurately distinguishes the harm alleged in *CompuServe*. *Intel* characterizes the harm from the emails in *CompuServe* as related to "*the functioning of CompuServe's electronic mail service*" and not, as in *Intel*, "about *the contents of the messages*," *id.* at 307, but the unsolicited commercial content of the messages is arguably a but-for cause of the customer's complaints in *CompuServe*.

If one focuses only on rival harm in the form of server congestion,[64] the holdings in *CompuServe* and *Intel* may tell an optimistic and rational story: They offer a form of rough justice with the more burdensome and congestive use that realistically threatens to impose actual rival harm resulting in an injunction. If one focuses on the speech involved, however, these holdings may equally offer a less appealing form of rough justice in which the courts use the harm requirement of cybertrespass as a proxy to reflect the courts' determination of the value of the speech. An information policy regime that vests in the courts the right to determine when information can and cannot flow based on the courts' subjective valuation of whether the content of the transmission amounts to harm is a regime that neither the server owners nor the information transmitters should support.

b. Extraction Cases

The facts of *eBay v. Bidder's Edge*[65] are illustrative of the extraction cases. A now well-known staple of e-commerce, plaintiff eBay uses a server to host an auction website—a forum for private sellers to set up and private buyers to bid in online auctions. The eBay server stores information on the products entered by the sellers and on the bids entered by the buyers, and it transmits this information to Internet users in the form of a web page whenever requested to do so. Defendant Bidder's Edge ran an auction-aggregator website—an information forum displaying the status of auctions being conducted on auction websites, including eBay—that permitted potential auction participants to comparison-shop. To collect its information in a timely fashion, Bidder's Edge used "spiders" or automated software programs that "crawled" or recursively queried all accessible pages of an auction site to glean the relevant data. After initially authorizing the Bidder's Edge spiders and then unsuccessfully attempting to negotiate a licensing agreement, eBay notified Bidder's Edge that its spiders were unwelcome and filed suit. The *eBay* court granted a preliminary injunction based on trespass to chattels that enjoined the Bidder's Edge spiders from accessing eBay's server.

eBay demonstrates that although cybertrespass technically addresses only invasions to a server, server owners may use it to control not only information

[64] Another definition of the harm requirement considered in *CompuServe* required rival use of a scarce resource, but expanded the relevant resource beyond the server to include the metered time of CompuServe's customers who received the email messages. *CompuServe*, 962 F. Supp. at 1023 ("[T]he receipt of a bundle of unsolicited messages at once can require the subscriber to sift through, at his expense, all of the messages to find the ones he wanted or expected to received."). The lower court in *Intel* also decoupled rival harm from the processing capacity server, holding the harm requirement satisfied because "e-mails caused disruption to Intel's workers, who were drawn away from their jobs to deal with the messages," Intel Corp. v. Hamidi, 114 Cal. Rptr. 2d 244, 251 (Cal.App.4th 2001), and because Intel employees spent time attempting to block Hamidi's email, *id.* at 250 (finding that Intel's business was "hurt by . . . the time its security department spent trying to halt the distractions"). The California Supreme Court, however, declined to recognize rival harm decoupled from the server. *Intel*, 71 P.3d at 308 ("It is circular to premise the damage element of a tort solely upon the steps taken to prevent the damage."). Decoupling of rival harm from the server effectively vitiates the harm requirement just as potential rival harm does.

[65] 100 F. Supp. 2d 1058 (N.D. Cal. 2000). The following factual description is derived from the *eBay* opinion. *See id.* at 1060-63.

"pushed" or distributed onto a server, but also information "pulled" off of, or extracted from, a server. Information from a website is downloaded—that is, copied from the server to a client—only after a client's signal requesting the information has been received.[66] To prevent competitors from mining and extracting the information it has made available to the general public on its server, eBay, like the other server owners in the extraction cases, uses a doctrine capable of excluding the "dumb" incoming signals to control the information-laden outgoing signals.

Server owners benefit from cybertrespass because they can use the tort to exercise control over how the information made available on their websites can be used. In all of the extraction cases, the defendants used the information copied from the server in ways that extended the server owner's rights under copyright and other intellectual property or unfair competition laws. In *eBay*, for example, the court noted that the "bulk of eBay's moving papers and declarations" addressed the violation of its information-based rights,[67] suggesting that, as in *Thrifty-Tel*,[68] the court resolved an issue that the server owner initially perceived as a problem concerning the use of its information with a property doctrine sounding in tangible property. eBay sought to suppress competition by controlling the copying and use of product and pricing information about its ongoing auctions—factual information that likely can be copied under copyright[69] and misappropriation[70] and that is not protected in the United States by database-specific legislation[71]—and preventing use of its trademark[72]—a use that might have been permissible under trademark law.[73]

[66] *Cf.* Reno v. ACLU, 521 U.S. 844, 869 (1997) (noting that "communications over the [World Wide Web] do not 'invade' an individual's home or appear on one's computer screen unbidden" and that "[u]sers seldom encounter content 'by accident'" (quoting ACLU v. Reno, 929 F. Supp. 824, 844 (E.D. Pa. 1996))).

[67] *eBay*, 100 F. Supp. 2d at 1063 n.6.

[68] *See supra* Section III.A.

[69] *See* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 344-45 (1991) ("That there can be no valid copyright in facts is universally understood."). *But cf.* O'Rourke, *Shaping Competition on the Internet: Who Owns Product and Pricing Information?*, *supra* note 4, at 1986-88 (arguing that the copying of unprotected information may also copy either distinct and protected information or a protectible selection or arrangement of unprotectible facts).

[70] *Cf.* O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, *supra* note 4, at 585-86 (arguing that web-based information aggregators are unlikely to be liable under the misappropriation doctrine).

[71] Congress has been considering a bill to protect databases for many years but has to date failed to pass one. *See, e.g.*, Jonathan Band & Makoto Kono, *The Database Protection Debate in the 106th Congress*, 62 OHIO ST. L.J. 869 (2001). Whether database protection is good information policy has generated much commentary. *See generally* Jane C. Ginsburg, *Copyright, Common Law, and Sui Generis Protection of Databases in the United States and Abroad*, 66 U. CIN. L. REV. 151 (1997); J.H. Reichman & Pamela Samuelson, *Intellectual Property Rights in Data?*, 50 VAND. L. REV. 51 (1997); Stephen M. Maurer & Suzanne Scotchmer, *Database Protection: Is It Broken and Should We Fix It?*, 284 SCIENCE 1129 (1999).

[72] *See eBay*, 100 F. Supp. 2d at 1063 & n.6, 1064 (noting that *eBay* had focused on a trademark infringement claim).

The other extraction cases involve similar factors: first, Internet users seeking to copy from a website (and thus from a server) information that is arguably in the public domain, or to use the information in a manner that is likely permissible under intellectual property rights and encouraged by their animating policies; and second, server owners who would benefit from preventing the copying and controlling of the information. Like *eBay*, *Ticketmaster Corp. v. Tickets.com, Inc.* involved a defendant who sought access to product and pricing information.[74] *Register.com, Inc. v. Verio, Inc.* involved a list of domain name registrants that the server owner was required to make freely available to the public, but that could provide a competitive advantage if not available to the business-competitor defendant in particular.[75] In *Oyster Software, Inc. v. Forms Processing, Inc.*, an Internet user sought to copy and aggregate trademark names used as metatags from a number of different servers and to use that information in a manner that is arguably permissible under the trademark laws.[76]

Like the distribution cases, the extraction cases do not recognize information harm directly, but they propose widely disparate notions of actionable rival harm, and the cases that find potential rival harm to be sufficient permit the server owners to vindicate information harm in substance if not in name. eBay received its requested preliminary injunction, the court's holding oscillating between an outright acceptance of potential rival harm[77] and a seemingly stiffer requirement imposing a

[73] *See* New Kids on the Block v. News Am. Publ'g, Inc., 971 F.2d 302, 306, 308 (9th Cir. 1992) (describing permissible nominative and fair uses of trademarks).

[74] No. 99CV7654, 2000 WL 1887522 (C.D. Cal. August 10, 2000), *aff'd*, No. 00-56574, 2001 WL 51509 (9th Cir. 2001). Ticketmaster owned a server and used it to sell tickets to concerts and performances. In addition to selling some tickets, Tickets.com aggregated concert-related information, employing spiders to crawl, among others, the Ticketmaster site, displaying the information on the tickets so retrieved on its own website, and allowing customers to link to the Ticketmaster website to purchase the tickets. *Id.*

[75] 126 F. Supp. 238 (S.D.N.Y. 2000), *aff'd* 356 F.3d 393 (2d Cir. 2004). The plaintiff Register.com, a domain name registrar, registered Internet users' requests for new domain names and maintained a WHOIS database of basic identity and contact information about the domain name registrants. The information in the database had to be publicly available according to Register.com's contract with ICANN. The defendant Verio, a designer and manager of web sites, repetitively queried this entire database to extract the names of and contact information for recent registrants. These recent registrants are the most valuable potential customers for website designers. *See id.* at 243 (noting Verio's moniker "Project Henhouse" for the information-gathering operation). Because Register.com also provided website design services, it could gain a competitive advantage by excluding Verio from the database. *Id.*

[76] No. C-00-0724 JCS, 2001 WL 1736382, *1-*2 (N.D. Cal. Dec. 6, 2001). Metatags are software-encoded words assocated with websites that search engines use to classify a site. *See* Brookfield Communications, Inc. v. W. Coast Entm't, 174 F.3d 1036, 1045 (9th Cir. 1999). The use of party A's trademark as a metatag for party B's website is permissible under certain factual conditions. *See, e.g.*, Playboy Enter., Inc. v. Welles, 279 F.3d 796, 803-04 (9th Cir. 2004) (permitting a former Playboy Playmate of the Year to use the registered trademarks "playboy" and "playmate" as metatags without authorization).

[77] *eBay*, 100 F. Supp. 2d at 1071 ("Even if, as [Bidder's Edge] argues, its searches use only a small amount of eBay's computer system capacity, [Bidder's Edge] has nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes.

hybrid rival harm standard and requiring the server owner to argue that future congestion is likely to occur.[78] *Ticketmaster* represents the harm requirement's high-water mark in the extraction cases: the court denied Ticketmaster's preliminary injunction, looking for actual rival harm to the server—"physical harm to the chattel" or "some obstruction of its basic function"—and finding none.[79] In contrast, the district court in *Register.com* held that property in networked servers encompassed the right to exclude all invading signals, granting Register.com's motion for a preliminary injunction based on a theory that the potential for rival harm to the server constituted actionable harm.[80] Likewise, in *Oyster Software* the court refused to dismiss the trespass claim because use of a resource that could, under certain conditions, impose congestion costs on other users was sufficient to satisfy the harm requirement, regardless of whether those conditions existed.[81]

The law recognizes no such right to use another's personal property. Accordingly, [Bidder's Edge]'s actions appear to have caused injury to eBay and appear likely to continue to cause injury to eBay."); *id.* ("eBay's claim is that [Bidder's Edge]'s use is appropriating eBay's personal property by using valuable bandwidth and capacity, and necessarily compromising eBay's ability to use that capacity for its own purposes.").

[78] The court noted that if it were to hold that Bidder's Edge did not cause actionable harm to eBay,

> it would likely encourage other auction aggregators to crawl the eBay site, potentially to the point of denying effective access to eBay's customers. If preliminary injunctive relief were denied, and other aggregators began to crawl the eBay site, there appears to be little doubt that the load on eBay's computer system would qualify as a substantial impairment of condition or value.

Id. at 1071-72. Even this stronger formulation of the harm requirement, however, was satisfied despite the fact that eBay made only a bare allegation without empirical evidence (and offered a convincing narrative) that future congestion was likely. *Id.* (noting only that "there appears to be little doubt" that actual rival harm would occur in the future).

[79] 2000 WL 1887522, at *4 ("It is noted that the harm to the equipment foreseen was to its intended function, not the physical characteristics of the computer. A basic element of trespass to chattels must be physical harm to the chattel (not present here) or some obstruction of its basic function (in the court's opinion not sufficiently shown here).").

[80] 126 F. Supp. 2d 238, 250 (S.D.N.Y. 2000) (concluding that "mere possessory interference is sufficient to demonstrate the quantum of harm necessary to establish a claim for trespass to chattels"); *id.* at 249 (noting that Register.com's testimony on harm to its computer systems was "thoroughly undercut"). In its brief treatment of the issue, however, the Second Circuit upheld the district court's preliminary injunction, emphasizing a likelihood-of-future-harm standard similar to the standard articulated in *eBay*. Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 404 (2d Cir. 2004) (attributing to the district court the finding "that Verio's use of search robots . . . consumed a significant portion of the capacity of Register's computer systems" and noting that "it was 'highly probable' that other Internet service providers would devise similar programs to access Register's data, and that the system would be overtaxed and would crash").

[81] 2001 WL 1736382, at *13 ("While the *eBay* decision could be read to require an interference that was more than negligible (as the court did in *Ticketmaster*), this Court concludes that *eBay*, in fact, imposes no such requirement. Ultimately, the court in that case concluded that the defendant's conduct was sufficient to establish a cause of action for trespass not because the interference was 'substantial' but simply because the defendant's conduct amounted to 'use' of Plaintiff's computer."). Oyster conceded that the invasion

IV. TRESPASS TO DOCUMENTS

One reason why cybertrespass litigation remains mired in the Restatement's historical morass is because courts have presumed that trespass to chattels and its harm requirement drifted into a legal backwater early in the twentieth century, reemerging only in the cybertrespass cases.[82] In part, I believe that the courts shied away from a robust harm requirement in the extraction cases because they discounted its contemporary relevance. The line of cases in which the harm requirement appears often involves the adjudication of property interests in domesticated animals[83] and understandingly seems antiquated. Trespass to land, by contrast, is a vibrant doctrine and has been used to suggest that the harm requirement should be reduced to a formality and should, for all practical purposes, disappear from cybertrespass.[84]

This section examines several cases never presented to the cybertrespass courts that mark a doctrinal road not taken: trespass to documents. These trespass-to-document cases are real-space analogs of the extraction case-type. They define the scope of property rights in a real-space information infrastructure—paper—as document owners sue information publishers under the theory that the publishers or their agents committed trespass to a document to obtain the information eventually published. Unlike in the majority of the cybertrespass extraction cases, however, the courts have frequently construed the harm requirement in trespass to documents in a robust fashion. With the social utility of disclosure of the information on one side of the scale and the defendants' property interest in their chattel on the other, courts have held that the limitations on information-based rights that foster the free flow of information should not be eclipsed by perfect propertization of the tangible good on which the information resides.

The Supreme Court's landmark decision in *Harper & Row, Publishers, Inc. v. Nation Enterprises*,[85] read in conjunction with the Second Circuit opinion it reversed,[86] is the most prominent of these trespass-to-document cases. In *Harper & Row*, the Supreme Court held that an article in The Nation magazine, which quoted a soon-to-be-published memoir by President Gerald Ford without the consent of the memoir's publisher, Harper & Row, constituted copyright infringement.[87] To arrive at this conclusion, the Court held both that The Nation had committed a prima facie

"placed a 'negligible' load on Oyster's computer system," but the court considered this fact irrelevant to its holding. *Id.*

[82] *See, e.g.*, Intel Corp. v. Hamidi, 114 Cal. Rptr. 2d 244, 247 (Cal. Ct. App. 2001) ("Trespass to chattels is somewhat arcane and suffers from desuetude . . . . However, the tort has reemerged as an important rule of cyberspace.").

[83] *See, e.g.*, Intel Corp. v. Hamidi, 71 P.3d 296, 323-24 (Cal. 2003) (Brown, J., dissenting).

[84] *See supra* note 8 (noting that trespass to land has been used to argue in favor of reducing the harm requirement in trespass to chattels to an easily satisfied formality).

[85] 471 U.S. 539 (1985).

[86] Harper & Row, Publishers, Inc. v. Nation Enters., 723 F.2d 195 (2d Cir. 1983).

[87] *Harper & Row*, 471 U.S. at 542-43.

violation of Harper & Row's exclusive right to publish the memoir, and that the quotation was not excused as a fair use.[88]

Regardless of the Court's eventual holding, the fair use analysis provided a doctrinal forum for the Court to weigh the overall social costs and benefits of The Nation's conduct in its factual context.[89] Fair use "permits courts to avoid rigid application of the copyright statute when, on occasion, it would stifle the very creativity it is designed to foster,"[90] and thus acts as a finely regulated safety valve to ensure that the exclusive rights granted by copyright do not catch the most socially productive uses of information in the net established to restrain counterproductive free-riding behavior. Fair use is perhaps the most commonly cited instance in which intellectual property demonstrates its nature as a balance between public rights to access and use and private rights to exclusive use.

But for a robust interpretation of harm requirement in trespass to chattels, however, the doctrinal forum in which this context-dependent fair use analysis occurred would not have been open to the Court. In its argument before the Second Circuit, Harper & Row claimed that The Nation's transitory use of one copy of the document from which the quotes were taken constituted a trespass to the document.[91] The Second Circuit rejected this argument, enforcing a harm requirement as an element of trespass to chattels and dismissing the trespass claim.[92] Harper & Row "could not succeed on this [trespass to chattels] claim . . . since liability for trespass to chattels exists only upon a showing of actual damage to the property interfered with."[93]

Had the Second Circuit held otherwise, reduced the harm requirement to a formality satisfied by a demonstration of potential harm through the transitory unavailability of the document, and granted Harper & Row a right to vindicate a possessory interest in the inviolability of the document, an absolute property right in the document-as-chattel would have foreclosed the fair use analysis. The limited

[88] *Id.* at 548-49, 569. Fair use is an affirmative defense to copyright infringement. *See* 35 U.S.C. § 107 (2001).

[89] In *Harper & Row*, the Court considered factors that related to the nature of both the infringed work—for example, that the memoir was a predominantly factual work, 471 U.S. at 563, and that it was unpublished, *id.* at 564—and the infringing use—for example, that the article was both an example of news reporting and a commercial venture, *id.* at 561-63, that it excerpted highly expressive passages, *id.* at 563-64, 565, and that it scooped an intended serialization of the memoir, *id.* at 566-68.

[90] Dr. Seuss Enters., L.P. v. Penguin Books U.S.A., Inc., 109 F.3d 1394, 1399 (9th Cir. 1997); *see also* Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 575 (1994) ("From the infancy of copyright protection, some opportunity for fair use of copyrighted materials has been thought necessary to fulfill copyright's very purpose, '[t]o promote the Progress of the Science and useful Arts . . . .'" (quoting U.S. Const., Art. I, § 8, cl. 8)).

[91] *See* Harper & Row, Publishers, Inc. v. Nation Enters., 723 F.2d 195, 201 n.5 (2d Cir. 1983).

[92] *Id.*

[93] *Id.* (citing HARPER & JAMES, *supra* note 37, § 2.15). The Second Circuit also addressed a conversion claim and found it, like the trespass to chattels claim, unsupportable as a matter of law. *See id.* at 199-201. The Supreme Court did not accept certiorari on either the trespass or the conversion issue.

propertization of the document on which the information was inscribed allowed the courts to inquire into the value of information-transforming conduct. Narrow infrastructure-based property rights were an important element in the overall array of doctrines that shaped information policy.

Another trespass-to-documents case, *Pearson v. Dodd*,[94] follows the same pattern as *Harper & Row*. In this case, the major difference is that the policy concerns supporting the free flow of information are given legal effect not through limitations on intellectual property but rather though limitations on causes of action for the invasion of privacy. In *Pearson*, a third party, without Senator Dodd's authority or knowledge, "entered [his] office . . . , removed numerous documents from his files, made copies of them, replaced the originals, and turned over the copies" to Pearson, "who was aware of the manner in which the copies had been obtained."[95] Based on the information in these documents, Pearson published articles that "expos[ed] the alleged misdeeds of Senator Thomas Dodd."[96] Angered by how he was portrayed in the articles, Senator Dodd sued Pearson for monetary damages.[97] Senator Dodd asserted two types of claims. First, he brought an information-based claim premised on the nature of the information included in the article, arguing that Pearson tortuously invaded his privacy.[98] Second, he brought an infrastructure-based claim premised on his property rights in the physical document in his office, arguing that Pearson was liable for conversion because the third party converted the documents when he copied them.

The district court ruled that Senator Dodd's property rights in the physical document had been violated: It granted summary judgment in favor of Senator Dodd on the liability aspect of the conversion claim, while granting summary judgment in favor of Pearson on the privacy claim because "the publications relate to [Senator Dodd's] activities as a high-ranking officer . . . in which the public has an interest."[99] The D.C. Circuit upheld the district court's ruling on the privacy claim,[100] but reversed on the conversion claim.[101] Importantly, it also addressed and dismissed

[94] 410 F.2d 701 (D.C. Cir. 1969).

[95] *Id.* at 703. Technically, the documents were turned over to Pearson's agent. *Id.*

[96] *Id.* The articles pertained to Senator Dodd's "relationship with certain lobbyists for foreign interests." *Id.*

[97] The district court had denied Senator Dodd's request for a preliminary injunction barring the publication of the information in a previous opinion that was not on appeal. Liberty Lobby, Inc. v. Pearson, 261 F. Supp. 726, 728 (D.D.C. 1966).

[98] The district court characterized the privacy claim as a claim about the nature of the published information. *See* Dodd v. Pearson, 279 F. Supp. 101, 105 (D.D.C. 1968) (addressing whether "the publication of the material of which the plaintiff complains is not protected by the cloak of the right of privacy"). The court of appeals, however, characterized the privacy claim as a claim about the manner in which the information was obtained, not about the contents of the information published. *See Pearson*, 410 F.2d at 704 (stating that the right to privacy claim pertained "rather to the manner in which the information in the [articles] was obtained than to the matter contained in them").

[99] *Dodd*, 279 F. Supp. at 105.

[100] *Pearson*, 410 F.2d at 703-06.

[101] *Id.* at 706-08.

Pearson's liability under a trespass-to-chattels theory because Senator Dodd could not satisfy the harm requirement. Senator Dodd could not make "a showing of actual damage to the property [i.e. the documents] interfered with."[102] "A theory of trespass to chattels [requires] an undisputed showing of actual damages to the property in question."[103]

Thus, like the Second Circuit in *Harper & Row*, the D.C. Circuit in *Pearson* refused to construe a property interest in a tangible document as a right that trumps the limitations in causes of action granting a private individual control over the flow of information:

> [Senator Dodd] complains, not of the misappropriation of property bought or created by him, but of the exposure of information either (1) injurious to his reputation or (2) revelatory of matter which he believes he has a right to keep to himself. Injuries of this type are redressed at law by suit for libel and invasion of privacy respectively, where defendants' liability for those torts can be established under the limitations created by common law and by the Constitution.[104]

The scope of the document owner's rights was restricted because the harm requirement in trespass to documents was interpreted in a substantive fashion. A cause of action alleging information harms had to be decided on the merits by information-oriented laws and the "limitations" therein, not by the laws that structure rights in tangible property.[105]

V. THE LESSON OF TRESPASS TO DOCUMENTS FOR CYBERTRESPASS

In some obvious ways, the parallel between the trespass-to-documents cases and the extraction cybertrespass cases is precise. Both involve infrastructure owners who seek to control the flow of information. Both question the appropriate scope of a property right in a tangible infrastructure on which information is inscribed. Furthermore, both frame the property question as one that is answered by the harm requirement in trespass to chattels. A robust harm requirement that looks beyond information harm and potential rival harm prevents the property rights in the infrastructure from controlling how someone who accesses the infrastructure to obtain information may subsequently use that information. A harm requirement that is reduced to a mere formality, however, grants the infrastructure owner control over the subsequent uses of information that do not even occur on the infrastructure itself.

[102] *Id.* at 707 (citing HARPER & JAMES, *supra* note 37).

[103] *Id.*

[104] *Id.* at 708.

[105] *See also* Birnbaum v. United States, 588 F.2d 319, 326 n.14 (2d Cir. 1978) (holding the "surreptitious opening and reproduction of letters without appropriating or physically damaging them" does not demonstrate the "dispossession or impairment" required to prove a cause of action in trespass to chattels and proceeding to a privacy analysis). *But see* Poff v. Hayes, 763 So.2d 234, 238-39 (Ala. 2000) (holding a brief dispossession of plaintiff's credit-card receipts, business records and accounting ledgers by defendant for the purpose of photocopying and showing to state bar to allege unethical practices amounted to actionable harm under trespass to chattels).

If one focuses on these parallels, the divergent results are surprising. In the real-space trespass to documents cases, the courts have opted for a robust harm requirement, whereas in extraction-type cybertrespass cases, the courts have tended to a more formalistic, peppercorn interpretation of the harm requirement.

This direct comparison does not, however, draw the most appropriate lesson for cybertrespass from the trespass-to-documents cases. The value of trespass to documents as persuasive precedent should not be overstated because neither the factual scenarios in the on-line and off-line worlds nor the policy concerns that these divergent factual scenarios raise are completely analogous. Briefly, I note three of these differences.

First, I believe that the document owner has a *stronger* equitable argument for property rights than the server owner does because the server owner has posted information in a publicly accessible location. The information at issue is not information that the website owner has sought to keep secret. The infrastructure in which property rights are claimed is an infrastructure chosen expressly to promote the dissemination of information to the public. What the server owner objects to is not public access to the server, but the access of particular individuals who use the information in a manner that the server owner believes is detrimental to his interests. In contrast, the document owner in the trespass-to-documents cases has made no such affirmative representation that the infrastructure is open to public use. To the extent that a property owner's rights to control conduct enabled by the propertized resource are limited by his decision to open the resource to the public for general use,[106] the cybertrespass cases, but not necessarily the trespass-to-documents cases, should result in a property right of only limited scope.

Second, the trespass-to-documents cases involve the question of liability for monetary damages for the information harm that the document user inflicts on the document owner.[107] In contrast, the server owners usually seek injunctive relief barring future trespasses. (The initial server access is not actionable because, at that time, the server owner was a member of the invited general public.[108] It is not until after the server owner expressly revokes consent that accessing the website becomes a trespass.) Server owners understand cybertrespass to be a way to control future action, to control ongoing uses of information that they have generated and made available to the public.[109]

[106] *See supra* notes 28-29 and accompanying text (discussing the general principle in property law that the more one opens the resource governed by private property rights to the public, the more the private property owner curtails his ability to use his right to exclude in a discriminatory fashion).

[107] *See supra* notes 44-47 and accompanying text (distinguishing information and rival harm in the cybertrespass cases).

[108] *But see supra* note 25 (suggesting that the original scope of the invitation to the public was limited).

[109] This limitation on the protection for information that a server owner may obtain through cybertrespass suggests that cybertrespass in its raw form will be most effective when repetitive access is required and thus when the information posted is dynamic.

Third, the physical nature of a networked server's information infrastructure—or the Internet's architecture, as Professor Lessig would say[110]— differs radically from the nature of the ream of paper on which a document is printed. This difference makes the right to exclude from a networked server a far more valuable tool for protecting publicly available information than the right to exclude from documents is in real space. To understand this difference, it is important to realize that although the Internet is frequently heralded as a social phenomenon that decentralizes access to information,[111] it is equally as much a technological phenomenon that centralizes the storage of the widely accessible information. A networked server allows a large and anonymous group of individuals to access information from a single chattel,[112] and property rights in that single chattel may therefore be used to put conditions on the subsequent uses to which that entire group may put the information.[113] May these individuals publish it (provided that they do not use the protected original expression if that expression is copyrighted)? May they use it to compete with the server owner? May they modify it? May they criticize it?

In real space, however, not everyone can read the same book, so authors and other compilers of information seeking to obtain widespread distribution of the information usually replicate the inscription in a large number of discrete books. The first-sale doctrine of copyright[114] effectively prevents the authors from claiming any property rights in the books-as-chattels once they are sold.[115] This is the real-space baseline: Authors lack a property right in the media in which information is inscribed. The trespass-to-documents cases implicate only the exception to this rule—when an information user gleans information from a document that is still in the possession of the author. Notably, the courts' substantive interpretation of the harm requirement in trespass to documents demonstrates that even in this exceptional

[110] *See generally* Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661, 662-64 (1998) (discussing architecture as one of four regulators of human behavior).

[111] *See, e.g.*, M. Ethan Katsh, *Rights, Camera, Action: Cyberspatial Settings and the First Amendment*, 104 YALE L.J. 1681, 1705 (1995) (arguing that "[p]lacing information into electronic form not only liberates the information from its pages but removes the need for specialized [real-space] spaces to hold particular kinds of information").

[112] I leave aside here the complicated issue presented when the contents of a web server are mirrored on a different server.

[113] I also leave aside there the possibility of one party accessing the server and passing the information on to a different party who engages in the use. Although the accessing party may be enjoined, it is possible that the using party could recruit a large enough group of accessers that cybertrespass would prove to be an ineffective legal technique of protecting information. This leakiness inherent in cybertrespass as a means of protecting information, however, is in part plugged up because cybertrespass will be most effective at protecting dynamic information, *see supra* note 109 and accompanying text, and such rapidly changing information is difficult to obtain in a reliable and timely fashion through intermediaries.

[114] *See* 17 U.S.C. § 109(a) (codifying the first-sale doctrine).

[115] Software shrink-wrap licenses that accompany the physical transfer of a disk, however, present an example of how the protections afforded by the first-sale doctrine may be weakened. *See generally* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996). Dust-jacket licensing in the publishing industry, however, has not yet become a common industry practice.

circumstance, property rights in real-space information infrastructures cannot be used to control the flow of information.

In conclusion, I believe that the trespass to document cases operate best as a simple reminder of exactly this point. Historically, property in chattels on which information is inscribed has deferred to intellectual property law. Both through the first sale doctrine and, as a back up, through the harm requirement in trespass to documents, it has been repeatedly tailored to prevent absolute property rights in the media from trumping the balance of public and private rights that animates intellectual property. Formally, cybertrespass may structure new-world information policy debates around classic, old-world questions of trespass and tangible property. However, it is in no way a proposal for the continuation of the status quo. Application of the old-world doctrine of trespass with which we are most familiar—the bright-line rule of exclusion—to that new world moves us away from, not towards, the balance of legal rights in real-space with which we are most familiar.[116]

[116] I do not believe that in a digital and networked world we must replicate the balance of public and private rights that previously existed merely because it is the balance with which we are today most familiar. The connectivity and automation possible in the networked world can be used to support arguments that digital information policy should be different and should allow an author to retain a greater amount of control over the uses to which the public may put information that the author has made available for public consumption. *See, e.g.*, William W. Fisher III, ***Property and Contract on the Internet***, 73 CHI.-KENT L. REV. 1203 (1998) (arguing for an overhaul of the copyright regime in a digital environment). These arguments, however, are most commonly formulated as arguments about contract and technological protections, not arguments about property in the tangible infrastructure of the Internet. If greater and more fine-grained control over information is the desired normative end, then cybertrespass in the extraction case-type is far too blunt an instrument to achieve this goal. *See supra* note 109 and accompanying text (noting that the extraction cybertrespass cause of action only allows the server owner to internalize the value of dynamic information).