RIGHTS OF ACCESS AND THE SHAPE OF THE INTERNET

MICHAEL J. MADISON*

Abstract: This Article reviews recent developments in the law of access to information, that is, cases involving click-through agreements, the doctrine of trespass to chattels, the anti-circumvention provisions of the Digital Millennium Copyright Act, and civil claims under the Computer Fraud and Abuse Act. Though the objects of these different doctrines substantially overlap, the doctrines yield different presumptions regarding the respective rights of information owners and consumers. The Article reviews those presumptions in light of different metaphorical premises on which courts rely: Internet-as-place, in the trespass, DMCA, and CFAA contexts, and contract-as-assent, in the click-through context. It argues that the different doctrines should be rendered consistent with one another and with an understanding of the relevant metaphor that is based on consumer and user experiences of the Internet, rather than on formal property-based constructs.

INTRODUCTION

When can the proprietor of a store of electronic information exclude unwanted users? When does the access granted to an invited user exclude unwanted use? These questions have challenged nearly a generation of scholars and lawyers.[1] The questions sounded first in computer software and later in electronic databases. They now also concern the contents of Internet Web sites and access to the Internet itself. For the practicing lawyer, solutions arrived first via boxtop and "shrinkwrap" licenses, later through "click-through" agreements, and still later as practical, legal, and metaphorical limits of those devices

* Assistant Professor, University of Pittsburgh School of Law. E-mail: madison@law.pitt.edu. Thanks to Dan Hunter, David McGowan, and participants at the Boston College Symposium on Intellectual Property, E-Commerce and the Internet, and the Chicago Intellectual Property Colloquium, for comments on earlier versions of this Article.

[1] The earliest commentary on shrinkwrap licenses appeared nearly twenty years ago. *See generally* David Einhorn, *The Enforceability of "Tear-Me-Open" Software License Agreements*, 67 J. PAT. & TRADEMARK OFF. SOC'Y 509 (1985); Richard H. Stern, *Shrink-Wrap Licenses of Mass Marketed Software: Enforceable Contracts or Whistling in the Dark*, 11 RUTGERS COMPUTER & TECH. L.J. 51 (1985).

emerged, through copyright law and its adjuncts, through property law, and through anti-hacking legislation. As the commercial lawyer now knows well, if undesirables cannot be excluded with contracts, they can be excluded under the Digital Millennium Copyright Act ("DMCA"), under the doctrine of trespass to chattels, and even under the Computer Fraud and Abuse Act ("CFAA").[2]

As Internet access-to-information issues arose, some metaphorical themes emerged. A consensus began to define the Internet as a virtual "place" or "space," or collection of "places" and "spaces," in many of the same terms that we conventionally use to describe our physical environment.[3] Electronic resources located "on" the Internet and more generally "in" tangible computer media have become commodities along with the media themselves, "things" to which one does or does not have access and that one can or cannot use. At the same time, in an apparently unrelated development, contract-law metaphors, and particularly the notion of "contract-as-assent," moved quietly online as a result of the extension of boxtop-license jurisprudence.[4] When one acknowledges receipt of a benefit with knowledge of limitations on use of that benefit, one "assents" contractually and is bound to the limitation.

The result is an uneven blend of doctrine and metaphor. From one perspective, issues of access to information, data, and computer programs became issues of access to the places, spaces, and things that constitute the Internet, a blend of two metaphors, one constituting "Internet-as-place," another constituting "information-as-thing."[5] Shrinkwrap and click-through jurisprudence developed around a second perspective using a different pair of metaphors, "information-as-thing" (still) but also "contract-as-assent."[6] The two perspectives yield

---

[2] *See* discussion *infra* Part II.B–D.

[3] *See* Mark A. Lemley, *Romantic Authorship and the Rhetoric of Property*, 75 TEX. L. REV. 873, 873–74 (1997) (noting competing metaphors, including "Information Superhighway," "Infobahn," "National Information Infrastructure," "cyberspace," and the term "Internet" itself). William J. Mitchell, Dean of the School of Architecture and Planning at MIT, wrote what remains the canonical discussion of the "place" metaphor in cyberspace in WILLIAM J. MITCHELL, CITY OF BITS: SPACE, PLACE, AND THE INFOBAHN (1995). Early legal scholarship pursuing this theme tended to focus on two issues. First, could the Internet be treated legitimately as a distinct jurisprudential "place"? *See* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1378–81 (1996). Second, when and how should the Internet be "zoned" by analogy to conventional zoning of cities? *See* Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1407–11 (1996).

[4] *See infra* notes 56–73 and accompanying text.

[5] *See infra* Part II.B–D.

[6] *See infra* notes 56–73 and accompanying text.

different doctrinal results in areas that substantially overlap. Click-through law has produced what appears to be a body of doctrine sensitive (mostly) to both producer and consumer interests. In part because its metaphorical underpinnings are weak, the present doctrinal equilibrium in this area is sensible yet tenuous.[7] Click-through jurisprudence (the pairing of contract-as-assent and information-as-thing metaphors) does not bind the legal analysis to any conventional understanding of how users experience the Internet or computer software. "Place" metaphors for the Internet, on the other hand, powerfully (if sometimes inaccurately) capture the experience of the Internet. So powerful are these metaphors that they largely have captured the imagination of legislators and judges, for whom the Internet-as-place metaphor connotes the absolute power of the property owner to exclude, and for whom a rule of "exclusion-from-computer" naturally assumes a rule of "exclusion-from-information." In short, click-through law draws the better doctrinal balance, based on actual use of the Internet, but the Internet-as-place metaphor tells the better story.

The problems here are twofold. The first is identifying the normatively "correct" balance between the right to control access to and use of presumptively private property, on the one hand, and two sorts of interests—legitimate interests in access and use without compensation, and interests in user awareness of limitations on access and use—on the other. This Article does not directly address the question of baselines, but it does argue that the default baseline now observed in practice under doctrines emphasizing Internet-as-place mistakenly applies a conclusive presumption that the "property" owner has an absolute right to exclude. Contract-based cases that place a greater burden on the "property" owner before granting such a power properly acknowledge, at least formally, that consumer interests must be weighed before recognizing a legal power to exclude.

---

[7] A recent decision of the U.S. Court of Appeals for the Federal Circuit appears to cast this conclusion into question. *See* Bowers v. Baystate Techs., Inc., 320 F.3d 1317, 1323–28 (Fed. Cir. 2003); *see also infra* note 109. Even before shrinkwrap licensing moved online, it was widely noted that the unwrapping of a package theoretically signified consumer "assent" to a shrinkwrap license, but practically speaking was meaningless to virtually all software users. A recent survey of click-through caselaw argues that the safer course, from the producer's standpoint, is to design the click-through mechanism so that the consumer cannot access the desired information without somehow affirmatively signifying assent to any access restrictions. *See* Christina L. Kunz et al., *Click-Through Agreements: Strategies for Avoiding Disputes on Validity of Assent*, 57 BUS. LAW. 401, 405–06 (2001).

The second problem is the inconsistency that results from applying these different bodies of law to essentially the same underlying phenomena. Click-through law suggests that an information user is not bound to limitations on information access without acknowledging those limitations. Trespass law, the DMCA, and the CFAA suggest otherwise. Thus, an online information proprietor that takes no steps to protect its data or copyrighted content may be better protected under the DMCA, the CFAA, or trespass doctrine—areas in which absolute property rules currently apply—than a producer that invests time, energy, and money in an enforceable click-through agreement. This is an odd result.[8] It is odd from the standpoint of the underlying policy goal that these doctrines share (that is, investments in efforts to produce and distribute intangible information should be legally protected as a way to preserve incentives to make those investments), odd from the standpoint of trying to distinguish genuinely anti-competitive uses of information products from benign uses, and odd from the standpoint of simple fairness.

What does this mean in practical terms? I argue below that shrinkwrap and click-through caselaw, the original line of argument regulating "access" to electronic places, has outlived the contract-as-assent metaphor on which it relies. Place metaphors rule. Trespass, DMCA, and CFAA cases so far suggest that courts have failed to appreciate the depth and complexity of the Internet-as-place metaphor, particularly in light of how users actually experience places on the Internet. If courts are going to rely on a place-based sensibility in evaluating claims that access to information should be restricted, they should do so in a way that not only applies that sensibility consistently across doctrinal lines, but also does so consistently with actual user experience.[9] The goal is not to provide a metaphorically consistent method for enhancing producer protection, nor to provide a meta-

---

[8] At the least, it defies the principal (and some would say, only) law of economics: there is no such thing as a free lunch.

[9] Reliance on "place" metaphors in common-law adjudication has not, therefore, necessarily "over-propertized" a common resource, in the property law sense, as some argue. *See, e.g.*, Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354 (1999) (showing how enclosure of information through laws supporting owners exclusive control pose risks to the diversity of our information environment). We have not necessarily lost access to public resources online. What we have lost is the ability to understand clearly what is accessible and what is not. The law has failed adequately to define the complexities of the interests that surround us. "Place," in legal practice, has an inappropriately flat dimension. That flatness inhabits relevant non-property regimes as well as property law.

phorically based argument for reviving the public domain. The goal is to balance those two interests in a consistent way as they engage one another across different doctrines. The Internet-as-place metaphor should be interpreted doctrinally in ways that are consistent with user experience of the Internet, rather than via formal, abstract, and absolutist notions of "property."

The argument proceeds as follows. Part I reviews the key metaphors involved in these doctrines and the links between metaphor and legal argument.[10] Part II reviews application and reliance on those metaphors in contract law, the law of property ("trespass to chattels") online, and related and parallel statutory developments, particularly the DMCA and the CFAA.[11] I argue that the common interests in "access" shared by these sources of law suggest that they be reconciled.[12] To the extent that their inconsistency derives from problems of metaphor, then either the latter group (trespass, the DMCA, and the CFAA) must be purged of the Internet-as-place metaphor, or the metaphorical gap in contract law needs to be filled. I am skeptical that "place" metaphors can be purged from Internet-related legal discourse. I argue, therefore, that the latter course is the better one. But what should that course consist of?

Part III introduces and describes the idea that in common usage our place metaphors invoke and depend on a specific type of place-based experience.[13] We inhabit, appreciate, and control our "places" by constituting mental "maps" of those places, relying on boundaries, landmarks, and other visible points of orientation. Part III argues that the legal developments described in Part II rely on an Internet-as-place metaphor but fail to leave us with comparable points of orientation.[14] We are left with a "place" that we do not understand and cannot properly control. The public interest is under-served in this scenario, and private interests cannot effectively rely on property rights

---

[10] *See infra* notes 17–50 and accompanying text.

[11] *See infra* notes 51–268 and accompanying text.

[12] *See infra* notes 51–268 and accompanying text.

[13] *See infra* notes 269–300 and accompanying text.

[14] An earlier version of this Article relied on the phrase "shotgun shack," in a title that began "Living in a Shotgun Shack," as a way of noting that metaphorically, we cannot tell whether the choices we make online lead us to a "shotgun shack" or a "beautiful house," phrases that the band Talking Heads once used to note the vast changes that may accompany life's small decisions. *See* TALKING HEADS, *Once in a Lifetime*, *on* REMAIN IN LIGHT (Sire Records 1980). The complete verse reads: "And you may find yourself living in a shotgun shack/And you may find yourself in another part of the world/And you may find yourself behind the wheel of a large automobile/And you may find yourself in a beautiful house, with a beautiful wife/And you may ask yourself—Well . . . How did I get here?" *Id.*

for needed incentives to invest and produce. Part IV suggests how some modifications in legal doctrine would bring it into closer harmony with the key metaphor.[15] This Part also briefly addresses objections to the proposal.[16]

I. METAPHOR AND ACCESS

This Part briefly defines some of the basic parameters of the Article as a whole, and it reviews the nature and the implications of three metaphors around which electronic "access" law has been organized.

The Article as a whole concerns the phenomenon of "access" to "information." I mean both of those terms in their broadest possible senses. I use the term "information" rather than the producer-oriented term "content" or the narrower "copyrighted material," because the cases and doctrines discussed touch on problems of controlled access in a variety of situations, from computer systems themselves to Internet service, to uncopyrightable databases, to copyrighted works.[17] I use the term "access" broadly and necessarily somewhat loosely (and am mindful that in other contexts the term has meanings and connotations that I do not wish to evoke)[18] to mean the ability of individuals to see, hear, understand, use, and in many cases reuse information content and/or services.[19]

Given these central terms, the four legal doctrines with which the Article is concerned revolve around three metaphors. These metaphors have played key roles in the development of the law of access. As noted above, they are "contract-as-assent," "information-as-thing," and "Internet-as-place." Each metaphor must be explained, but the significance of metaphor itself should first be noted, because the argument here is based on the premise that the language of legal doctrine makes a significant difference with respect to the organization and application of the doctrine.

---

[15] *See infra* notes 301–368 and accompanying text.

[16] *See infra* notes 352–363 and accompanying text.

[17] These situations would include both information and services apparently controlled by the user (software on the user's computer, or Internet service accessed by the user), as well as those owned or controlled by others.

[18] There are robust debates concerning "access" to various types of physical facilities, particularly access by competitors to incumbent telecommunications facilities for purposes of providing long-distance telephone service and for providing "access" to the Internet. *See generally* James B. Speta, *Handicapping the Race for the Last Mile?: A Critique of Open Access Rules for Broadband Platforms*, 17 YALE J. ON REG. 39 (2000).

[19] This necessarily includes the problem of access to information via computer program or robot.

Our use of language reflects the way in which we organize the world of our experience. Metaphor is more than a mere literary device. From a cognitive science perspective, "[m]etaphor is an expression forming a non-literal similarity comparison between two things, which has an expressive or affective content and thereby carries meaning."[20] A metaphor in this sense represents some typically more abstract cluster of concepts (the "target" domain) that is understood in terms of concepts from a typically more concrete, even physical area (the "source" domain).[21] Such a metaphor operates as a conceptual system that helps us understand the target, in which features are drawn from the source and applied to (or mapped onto) the target, rather than as a direct, literal correspondence of the two domains.[22] The mapped similarities between the two likewise carry meaning over from the source to the target.[23] To take a simple example, we often conceptualize our physical and emotional well-being in financial terms. An increase in well-being is a "gain" and thus good; a decrease is a "loss" or a "cost" and therefore harmful. An example familiar to lawyers is the metaphor corporation-as-person.[24] To cognitive scientists, this use of language and its structures not only influences the thoughts of speakers and affects our experiences with the world, but is itself reflective of our underlying cognitive structures, derived from experience.[25] Language,[26] and in particular metaphorical uses of lan-

---

[20] Dan Hunter, *Reason is Too Large: Analogy and Precedent in Law*, 50 EMORY L.J. 1197, 1209 (2001).

[21] *See id.* at 1209–10.

[22] *See id.*

[23] *See id.* at 1209–14 (describing the basic contours of cognitive science approaches to metaphor and its relative, analogy).

[24] *See generally* Sanford A. Schane, *The Corporation Is a Person: The Language of a Legal Fiction*, 61 TUL. L. REV. 563 (1987).

[25] *See* Hunter, *supra* note 20, at 1214–27 (summarizing cognitive science research on sources of mapping constraints). At one level, we may experience the world as we do, and behave in certain ways, because at some level our use of the semantics and syntax of our language predispose us to do so. In its strongest form, this argument is known as the Sapir-Whorf Hypothesis, after the two men most closely associated with it. *See* B.L. Whorf, *The Relation of Habitual Thought and Behavior to Language*, *in* LANGUAGE, CULTURE AND PERSONALITY 75–93 (Leslie Spier et al. eds., 1941). *See generally* EDWARD SAPIR, LANGUAGE: AN INTRODUCTION TO THE STUDY OF SPEECH (1949); EDWARD SAPIR, SELECTED WRITINGS OF EDWARD SAPIR (David G. Mandelbaum ed., 1949); BENJAMIN LEE WHORF, LANGUAGE, THOUGHT, AND REALITY: SELECTED WRITINGS OF BENJAMIN LEE WHORF (John B. Carroll ed., 1956). The "universalist" or strongest form of the hypothesis has been challenged on theoretical and empirical grounds. *See, e.g.*, STEVEN PINKER, THE LANGUAGE INSTINCT 59–67 (1994). The weaker form of the hypothesis, known as "linguistic relativity," argues that manners of speech influence habits of thought and behavior and has been supported in some experimental settings. *See generally* Paul Kay & Willett Kempton, *What Is the Sapir-*

guage,[27] are as reflective of thought and behavior as they are determinants. Metaphor contains unusual persuasive power because of its ability to tap into tacit but shared conceptual structures.[28] We talk as we do because of how we think and how we act.

> Most [semantic] categorization is automatic and unconscious, and if we become aware of it at all, it is only in problematic cases. In moving about the world, we automatically categorize people, animals, and physical objects, both natural and man-made. This sometimes leads to the impression that we just categorize things as they are, that things come in natural kinds, and that our categories of mind naturally fit the kinds of things there are in the world. But a large proportion of our categories are not categories of *things*; they are categories of abstract entities. We categorize events, actions, emotions, spatial relationships, social relationships, and abstract entities of an enormous range: governments, illnesses, and entities in both scientific and folk theories, like electrons and colds.[29]

Our semantic categories and our metaphors are not mere byproducts of (and inputs for) political debate. They are largely built on our experiences.[30]

Whorf Hypothesis?, 86 AM. ANTHROPOLOGIST 65 (1984); Alan Rumsey, *Wording, Meaning, and Linguistic Ideology*, 92 AM. ANTHROPOLOGIST 346 (1990). My argument does not directly rely on the Sapir-Whorf Hypothesis in either form, but there is a strong intuitive sense that our formal linguistic classifications influence our legal classifications. On the role of metaphor in shaping the law, see generally ANTHONY G. AMSTERDAM & JEROME BRUNER, MINDING THE LAW 189–92 (2000); STEVEN L. WINTER, A CLEARING IN THE FOREST: LAW, LIFE, AND MIND (2001).

[26] *See* GEORGE LAKOFF, WOMEN, FIRE, AND DANGEROUS THINGS: WHAT CATEGORIES REVEAL ABOUT THE MIND 58 (1987).

[27] *See, e.g.*, GEORGE LAKOFF & MARK JOHNSON, METAPHORS WE LIVE BY 3–6 (1980); GEORGE LAKOFF & MARK TURNER, MORE THAN COOL REASON: A FIELD GUIDE TO POETIC METAPHOR, at xi–xii (1989). A useful recent synthesis of research on metaphor and its application to legal reasoning is Thomas W. Joo, *Contract, Property, and the Role of Metaphor in Corporations Law*, 35 U.C. DAVIS L. REV. 779 (2002). On Lakoffian theory and the Internet in particular, see Dan Hunter, *Cyberspace as Place, and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439 (2003).

[28] *See* Hunter, *supra* note 20, at 1208–10; Joo, *supra* note 27, at 782–88; *see also* Lawrence Lessig, *The Regulation of Social Meaning*, 62 U. CHI. L. REV. 943, 958–61 (1995) (observing that social meanings draw power from uncontested or "invisible" expectations).

[29] LAKOFF, *supra* note 26, at 6.

[30] *See id.* at 330–34.

As language reflects our underlying experience, it likewise imports the normative implications of that experience.[31] Metaphor helps us to communicate effectively because it relies on devices the rhetorical validity of which are presumptively accepted in their cultural context.[32]

> For the same reasons that schemas and metaphors give us power to conceptualize and reason, so they have power over us. Anything that we rely on constantly, unconsciously, and automatically is so much part of us that it cannot be easily resisted, in large measure because it is barely even noticed. To the extent that we use a conceptual schema or a conceptual metaphor, we accept its validity. Consequently, when someone else uses it, we are predisposed to accept its validity.[33]

The benefit of metaphor derives therefore not only from communication of common conceptual structures, but also from the normative implications of those structures.[34] Metaphors in practice provide an organizing vocabulary that has normative power.[35] To describe one (difficult) thing in terms of another (easier) thing is not merely to argue that the first is *like* the second, though this is one possible use of metaphor. A metaphor in the form "source-as-target" suggests a manner of not only describing but also evaluating the source using descriptors and analyses developed for the target.[36] It is this use of metaphor with which this Article is concerned. In current access doctrines, there are three key metaphors of this type.

A. *Contract-as-Assent*

Contract law scholarship has collected a number of organizing schemas (contract-as-bargain, contract-as-relationship), and among these the formalist contract-as-assent metaphor has a respectable

---

[31] *See* LAKOFF & TURNER, *supra* note 27, at 62–65.

[32] *See id.*

[33] *See id.* at 63.

[34] *See id.* at 65 ("We not only import entities and structure from the source domain to the target domain, we also carry over the way we evaluate the entities in the source domain."); Pierre Schlag, *The Aesthetics of American Law*, 115 HARV. L. REV. 1047, 1051–54 (2002); Steven L. Winter, *Transcendental Nonsense, Metaphoric Reasoning, and the Cognitive Stakes for Law*, 137 U. PA. L. REV. 1105, 1143–46 (1989).

[35] *See* LAKOFF & JOHNSON, *supra* note 27, at 3–6.

[36] *See id.*

pedigree. The model has been well-defended and well-critiqued elsewhere.[37] Here, I wish only to point out the argumentative implications of the metaphor, which are developed in the cases discussed in the next Part. Contract-as-assent signifies that the parties' choices determine their legal obligations, that they in fact have choices to make, that they are capable of making those choices, and that their actions accurately reflect their choices. The metaphor may also imply that the parties are free from coercive influences, and that they possess information sufficient to enable them to make a choice. There is no doubt that this is a highly artificial and formal model.[38] As we see below, it appears to be the model of the moment.

B. *Information-as-Thing*

"Access" to information suggests, among other things, that there is an object of the access relationship, some*thing* to be obtained. Though "information" is an intangible, that intangible is necessarily commodified not only by virtue of being made the object of a commercial transaction, but also by virtue of the language that surrounds it.[39] We want access *to* information, an object. Objects are created, bought, sold, and even shared; these transactions become the substrate of broader regulation both of copyrighted and non-copyrighted "works" and of use of other electronic resources.[40] The influence of the information-as-thing metaphor appears, at least implicitly and occasionally explicitly, in both click-through and non-click-through access jurisprudence.

---

[37] *Compare* Randy E. Barnett, *A Consent Theory of Contract*, 86 COLUM. L. REV. 269 (1986) (defending consent model), *with* Richard Craswell, *Contract Law, Default Rules, and The Philosophy of Promising*, 88 MICH. L. REV. 489 (1989) (critiquing autonomy-based models of contract).

[38] *See* Melvin Aron Eisenberg, *The Emergence of Dynamic Contract Law*, 88 CAL. L. REV. 1743, 1759–60 (2000); Ralph James Mooney, *The New Conceptualism in Contract Law*, 74 OR. L. REV. 1131, 1177 (1995).

[39] It may also be commodified technologically. *See* Michael Buckland, *Information as Thing*, 42 J. AM. SOC. INFO. SCI. 351, 358 (1991).

[40] *Cf.* THE COMMODIFICATION OF INFORMATION, at vii–viii (Kluwer Law Int'l, Information Law Series No. 11, Niva Elkin-Koren & Neil Weinstock Netanel eds., 2002) (describing information as subject to the "rough and tumble of the marketplace" and copyright law as providing a legal groundwork for its propertization); Rochelle Cooper Dreyfuss, *Information Products: A Challenge to Intellectual Property Theory*, 20 N.Y.U. J. INT'L L. & POL. 897, 897–900 (1988). On the "thingification" of legal concepts, see Felix S. Cohen, *Transcendental Nonsense and the Functional Approach*, 35 COLUM. L. REV. 809, 811 (1935); Michael A. Heller, *The Boundaries of Private Property*, 108 YALE L.J. 1163, 1193–94 & n.162 (1999).

C. *Internet-as-Place*

Place and space metaphors for online interactions and environments are inescapable. Scholars have filled academic journals, and judges have filled opinions, with analyses of the "right" metaphor for the Internet,[41] without enduring success. Descriptively, however, as use of the Internet has increased and as it has become more embedded in different aspects of society at large, property-based descriptors have become well entrenched in both legal and popular usage.[42] It is difficult to conceive of educating Internet users today to stop using phrases such as "Uniform [or Universal] Resource *Locator*," "Web *site*,"

---

[41] *See, e.g.*, Taubman Co. v. Webfeats, 319 F.3d 770, 778 (6th Cir. 2003) ("The rooftops of our past have evolved into the internet domain names of our present. We find that the domain name is a type of public expression, no different in scope than a billboard or a pulpit . . . ."); Brookfield Communications, Inc. v. W. Coast Entm't Corp., 174 F.3d 1036, 1057 (9th Cir. 1999) (describing World Wide Web as "a marketing and advertising facility," and a "marketing and advertising tool"); Mainstream Loudoun v. Bd. of Trs. of the Loudoun County Library, 2 F. Supp. 2d 783, 793–94 (E.D. Va. 1998) ("[A] library must actually expend resources to restrict Internet access to a publication that is otherwise immediately available. In effect, by purchasing one such publication, the library has purchased them all. The Internet therefore more closely resembles plaintiffs' analogy of a collection of encyclopedias from which defendants have laboriously redacted portions deemed unfit for library patrons."); ACLU v. Reno, 929 F. Supp. 824, 836–37 (E.D. Pa. 1996) (describing World Wide Web as "a single body of knowledge"), *aff'd sub nom.*, Reno v. ACLU, 521 U.S. 844 (1997); A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 507 (1996) (suggesting rejection of "information ocean" metaphor in favor of "information fishbowl"); A. Michael Froomkin, *The Metaphor is the Key: Cryptography, The Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 859–80 (1995) (noting variety of metaphors used to describe cryptography and concerns embedded in choice of metaphor); Maureen A. O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 BERKELEY TECH. L.J. 561, 581–96 (2001) (comparing implications of "website as book" metaphor with "website as real property" metaphor); Alfred C. Yen, *Western Frontier or Feudal Society?: Metaphors and Perceptions of Cyberspace*, 17 BERKELEY TECH. L.J. 1207, 1208 (2002) (developing a cyberspace metaphor by analogy to feudal social relations). Maureen O'Rourke previewed some of the legal issues discussed in this Article in Maureen O'Rourke, *Fencing Cyberspace: Drawing Borders in a Virtual World*, 82 MINN. L. REV. 609, 654–701 (1998), arguing that the legal system needed to erect virtual "fences" on the Internet to preserve appropriate boundaries between intellectual property doctrines and related common law approaches.

[42] David Post and David Johnson argued in a seminal article in 1996 that unique, cross-border features of cyberspace meant that cyberspace *should* be characterized as a distinct place for purposes of legal analysis. *See* Johnson & Post, *supra* note 3, at 1370–80. Dan Hunter, who catalogues the manifest ways in which the Internet is treated as a metaphorical "place" by judges, argues that dislodging the metaphor is a central task facing judges and lawmakers but ultimately despairs of success. *See* Hunter, *supra* note 27. Mark Lemley, while agreeing with Hunter's diagnosis, offers some prescriptions for a partial cure. From his perspective, courts using analogical decisionmaking techniques have failed to appreciate the complexity of place and space in the off-line legal world. *See generally* Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521 (2003).

"*domain* name," "cyber*squatting*," "*home* page," or electronic mail "*address*." We describe the Internet in place and space terms in part because that is how we understand and experience it. "[N]o matter where you go . . . there you are," as the celluloid philosopher Buckaroo Banzai once said,[43] and it follows that wherever you "go" "on" the Internet, you sense that you are somewhere other than sitting in front of a computer monitor.[44] The argumentative vocabulary that this metaphor produces is relatively thin once we move beyond descriptions of Internet phenomena. Is the Internet really a metaphorical place? Or is it a metaphorical space?[45] Open (space), or bounded (place), or partly both? Even speaking metaphorically, is the Internet, or cyberspace, the correct target domain? Perhaps the World Wide Web, or Web sites, would be better.[46] In the cases and doctrines de-

---

[43] THE ADVENTURES OF BUCKAROO BANZAI ACROSS THE EIGHTH DIMENSION! (MGM Studios 1984).

[44] Johnson and Post describe the source of the usage as the persistence of information available on the Internet and the fact that this information is available broadly to large numbers of individuals. *See* Johnson & Post, *supra* note 3, at 1379. In the context of access to a Web site under the Federal Americans with Disabilities Act, however, at least one court has held that a Web site is *not* a place, at least under the terms of that statute. *See* Access Now, Inc. v. Southwest Airlines, Co., 227 F. Supp. 2d 1312, 1317 (S.D. Fla. 2002).

[45] Analyses of the "architecture" of the Internet coexist peaceably with analyses of the Internet as "place." *Compare* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 24–42 (1999) (analyzing the architecture of the Internet), *with* James Boyle, *The Public Domain: The Second Enclosure Movement and the Construction of the Public Domain*, 66 LAW & CONTEMP. PROBS. 33, 37–44 (2003) (analyzing the Internet as a "commons," that is, a "place"). The paradox that the Internet is simultaneously an environment (a place) and an object in that environment (a metaphorical building, which can be described in terms of its "architecture") may not matter for present purposes. In other contexts, emphases on the environmental attributes of the Internet may conflict with prescriptions for responsible (architectural) development.

[46] My concern in this Article is with what Yochai Benkler distinguished as the content "layer" of the Internet, rather than with its "logical" or physical "layers." Yochai Benkler, *From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access*, 52 FED. COMM. L.J. 561, 562 (2000). The analytic difficulty is that although one might distinguish physical machines, wires, and electrons (physical layer) from the software protocols that coordinate the activity of these machines and electrons (logical layer) from the information perceived on computer screens by end-users (subdivided by server, protocol, and Web site, among other things) (content layer), no one layer can be completely physically or analytically divorced from any other. Traditional lines between law and artifact, and text and machine, are being blurred. *See generally* Randal C. Picker, *From Edison to the Broadcast Flag: Mechanisms of Consent and Refusal and the Propertization of Copyright*, 70 U. CHI. L. REV. 281 (2003) (arguing that because access to information is no longer defined automatically by the character of the object in which the information is embedded, a re-assessment of policy and other access-regarding concerns is necessary); Margaret Jane Radin, *Online Standardization and the Integration of Text and Machine*, 70 FORDHAM L. REV. 1125 (2002) (describing implications of decline of traditional distinctions between intangible text and tangible machine); Dan L. Burk, DNA Rules: Legal Im-

scribed in the next Part, courts have supplied a place-based vocabulary that echoes the formalism of the contract-as-assent metaphor: "place" means property, property means private property, and private property means the owner's absolute right to exclude.

As these references to the property owner's "absolute right to exclude" suggest, metaphors bring risks as well as benefits. The most significant risk is that the metaphor will become unmoored from its conceptual underpinnings, and the linguistic formulation will be taken literally.[47] The institution of contract, and individual contracts themselves, are not truly constituted by assent alone. Authentic, subjective assent of each party need not be proved before a promissory obligation will be enforced.[48] Information as such is not a thing, although information can be collected and packaged in a commodified form.[49] The Internet is not really a place, nor is it really a parcel (or collection of parcels) of real property. Those features of the Internet that suggest to us that in some ways, it resembles a place should not be mistaken for evidence that the Internet is precisely like a place.[50] As the following analysis suggests, courts that describe the Internet

---

plications of Biological "Lock-Out" Systems (working paper, on file with author) (describing research of historians of science and technology). *But see* Julie E. Cohen, Lochner *in Cyberspace: The New Economic Orthodoxy of "Rights Management,"* 97 MICH. L. REV. 462, 531–32 (1998) (describing the "Cohen theorem," which states that consumers should have the right to hack technological rights management systems to defend privileges afforded traditionally by copyright law). For this reason, among others, I do not distinguish in this Article between "the Internet" and "cyberspace."

[47] Ian R. Kerr, *Mind Your Metaphors: An Examination of the Inefficacy Argument as a Reason Against Regulating On-Line Conduct*, *in* ETHICS AND ELECTRONIC INFORMATION IN THE TWENTY-FIRST CENTURY 231, 233–34 (Lester J. Pourciau ed., 1999) (updating an argument Lon Fuller originally offered in L.L. Fuller, *Legal Fictions*, 25 ILL. L. REV. 363 (1930)).

[48] *See* Randy E. Barnett, *Consenting to Form Contracts*, 71 FORDHAM L. REV. 627, 628–30 (2002); Joseph M. Perillo, *The Origins of the Objective Theory of Contract Formation and Interpretation*, 69 FORDHAM L. REV. 427, 427–29 (2000) (detailing the development of objective standards in contract formation).

[49] *See* Yochai Benkler, *An Unhurried View of Private Ordering in Information Transactions*, 53 VAND. L. REV. 2063, 2065–77 (2000); *see also* Dan Schiller, *How to Think About Information*, *in* THE POLITICAL ECONOMY OF INFORMATION 27, 32–33 (Vincent Mosco & Janet Wasko eds., 1988) (distinguishing between "information as resource," presumptively unowned and available to all, and "information as commodity," presumptively ownable and tradable).

[50] *See* GERTRUDE STEIN, EVERYBODY'S AUTOBIOGRAPHY 289 (1937) ("[T]here is no there there."); Lemley, *supra* note 42 (describing public goods attributes of informational content of cyberspace that distinguish it from tangible property); *cf.* Digital Equip. Corp. v. Altavista Tech., Inc., 960 F. Supp. 456, 462 (D. Mass. 1997) ("The Internet has no territorial boundaries. To paraphrase Gertrude Stein, as far as the Internet is concerned, not only is there perhaps 'no there there,' the 'there' is *everywhere* where there is Internet access.").

using place metaphors fundamentally err if they explicitly or implicitly assume that the Internet and cyberspace and all that it contains actually do consist of or operate precisely like real property.

The point of this Part has been primarily descriptive, to explain the role of metaphor in argument generally, and to identify the key metaphors at work in different doctrines regulating "access" to "information." There is an implicit normative critique, as well, previewing the argument of Part III: metaphors can mislead as well as describe, and metaphors can be persuasive in both misleading and accurate ways. As the next Part explains, in the click-through context, contract-as-assent coupled with information-as-thing produces a misleading but ultimately unpersuasive narrative. In the trespass, DMCA, and CFAA contexts, information-as-thing coupled with Internet-as-place produces a misleading result. The analysis focuses on the assent and place metaphors, treating the information-as-thing metaphor largely as a constant.

II. Managing Rights of Access: Click-Through Agreements, Trespass to Chattels, the DMCA, and the CFAA

This Part briefly surveys the history and current status of four sources of law that regulate access to information stored electronically, principally (but not exclusively) on computer networks: common-law contract law as applied to click-through agreements,[51] the common-law doctrine of trespass to chattels as applied to computer networks,[52] the DMCA,[53] and the CFAA.[54] Each of these bodies of law

---

[51] *See infra* notes 56–139 and accompanying text.

[52] *See infra* notes 140–183 and accompanying text.

[53] *See infra* notes 184–224 and accompanying text.

[54] *See infra* notes 225–268 and accompanying text. I do not separately discuss the proposed Uniform Computer Information Transactions Act ("UCITA") (2002), which, in those jurisdictions where it is in effect, specifically characterizes "licenses" for access to electronic information as contracts and validates the formation of such contracts via clickwrap and click-through mechanisms. The model UCITA proposal is available at http://www.law.upenn.edu/bll/ulc/ulc.htm#ucita. UCITA has been adopted wholly or partly in Maryland and in Virginia. Iowa, North Carolina, and West Virginia have adopted anti-UCITA "bomb shelter" legislation, which denies enforcement of contracts governed by UCITA against residents of those states. Sections 208 and 209 of UCITA permit the formation of contracts using shrinkwrap and click-through mechanisms, including mechanisms that require assent and payment for access before all terms are disclosed to the offeree. Sections 112 and 113 require that the offeree have an "opportunity to review" and to reject post-assent contract terms before such terms can be enforced, but the "opportunity to review" need not do more than bring the terms to the attention of a reasonable person.

has developed largely independently of the others, not entirely unaware of their related nature but nonetheless ill-equipped, based on the internal dynamics of their respective doctrinal objectives, to deal alone with the broader policy issues that they share.[55] The Part starts with a very brief history and overview of click-through contract law. In the Sections that follow this overview, I note the emergence of the Internet-as-place metaphor and the resulting shift to property-based doctrine. The corresponding change in doctrinal emphasis, from mutual assent to the interests of the property owner, leads to virtually no consideration of the ability of would-be defendants to avoid causing harm to the plaintiff. This framework is applied, moreover, in an electronic context (computer networks, and the Internet in particular) in which computer users have little or no ability to avoid inflicting the very type of harm that courts condemn.

A. *Click-Through Agreements*

"Click-through" agreements derive from "shrinkwrap" agreements. Shrinkwrap agreements took their name from software companies' practice of distributing boxed computer programs to customers under standardized terms that were "offered" on the face of, and sometimes inside, the boxes themselves.[56] These computer programs

---

[55] From the information producer or proprietor standpoint, the question is whether and how the proprietor can recover enough money via exploitation of the information or otherwise to preserve appropriate incentives to create and distribute information-related products. From the consumer or public standpoint, the question is whether and how to obtain and maintain some desirable level of access to and use of information-related products and information itself needed for industrial, cultural, community, political, and/or individual development. Each of the four bodies of law discussed in this Article has been used, at least in significant part, to manage perceived tradeoffs between those two points of view. Other sources of "access" law are not considered explicitly, but could be viewed as of a piece with these four. *See, e.g.*, Kelly v. Arriba Soft Corp., 280 F.3d 934 (9th Cir. 2002) (discussing law of hyperlinks).

[56] This account is adapted from Michael J. Madison, *Legal-Ware: Contract and Copyright in the Digital Age*, 67 FORDHAM L. REV. 1025, 1055–58 (1998). Whether terms stated on the outside of a package of computer software, or on a card inside the package, or provided during a download or installation process for software delivered via computer network, were reasonably understood by the user as an "offer" is a question that has never been thoroughly analyzed by a court. *Cf.* E. ALLAN FARNSWORTH, CONTRACTS § 4.26, at 298 (3d ed. 1999) (Courts may reject enforcement of a standardized contract form "on the ground that it was not of a type that would reasonably appear to the recipient to contain the terms of a proposed contract. Even under the objective theory, it can be reasoned that such a writing is not an offer at all."). Because virtually all of the debate has centered on the effectiveness of the user's alleged assent, sometimes characterized as the question of whether the user understood that the act of opening, clicking, or retaining amounted to an act of contractual significance, the summary and analysis that follow does so as well.

were typically delivered on diskettes or tapes packaged in book-sized boxes.[57] Because the boxed software was often not purchased from the software developer, proposing an "offer" in this way allowed the software developer, via distribution of the product by a third-party, to create the appearance of a direct contractual relationship between developer and end-user.[58] Customers "accepted" the terms of the agreements, according to the text of the agreements, by opening the plastic shrinkwrap packaging that encased the boxes.[59]

The combination of graphical user interfaces for software and delivery of computer software via computer networks led to the use of "shrinkwrap" agreements manifested in software itself rather than on cards or product packaging.[60] From the term "shrinkwrap," software companies developed the neologisms "click-wrap," "click-through," and "click-on" agreements.[61] Each of these terms today refers to mechanisms employed with respect to both pre-packaged computer software and databases, and software and data delivered via the Internet or other computer network, as to which the customer or end-user is permitted to access and/or use the program, service, or data only after "clicking" on one or more screen icons labeled "I Accept," "I Agree," or the like.[62] Click-through agreements frequently serve as the basis for two-party transactions, in addition to bridging gaps between two contracting parties separated by a third-party distributor.[63]

The shrinkwrap (and later click-through) mechanism developed to deal with the novelty of software companies' insistence that their copyrighted code was "licensed," rather than "sold" to each consumer, so that the companies were not required by the first sale doctrine to

---

[57] Madison, *supra* note 56, at 1055–56.

[58] *Id.*

[59] *Id.* Boxtop or "tear-me-open" licenses operated similarly. The customer "accepted" the offered terms by opening the box in which the software was delivered. License terms appeared on the top of the box. *See* Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239, 1241–45 (1995).

[60] Madison, *supra* note 56, at 1056–58.

[61] *Id.*

[62] *Id.* Some commercial lawyers distinguish between "click-wrap" (i.e., assent manifested by clicking on an "I Accept" or "I Agree" icon) and "click-through" or "click-on" agreements (i.e., assent to terms of use posted on a Web site home page that accompanies the installation of a computer program, manifested by clicking on a link to an interior page of a Web site). The term "browse-wrap" has also been used to refer to arguments by Web site owners that those who browse a Web site "agree" to Terms of Use posted on the site, merely by accessing the site. *See* Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 245–48 (S.D.N.Y. 2000).

[63] *See* Madison, *supra* note 56, at 1056.

give up their exclusive rights to distribute these works.[64] The mechanism, in other words, was expressly designed to require that the consumer (user) agree that "access" to the computer software was limited by the express terms of the license.[65] The license typically prohibited precisely the kinds of "access" that users of copyrighted works enjoy once they acquire a tangible "copy" of a copyrighted work.[66] If the program were installed on the first user's computer, that user might give or sell the medium (disk or tape) bearing the program to a second user, so that the second user could install the computer program on a second machine, while the first user retained use of the program on the initial machine. Assuming that the license limited use of the program to one user or one computer, the shrinkwrap license cut off unauthorized second points of "access."

From this perspective, the information proprietor's impulse to use a click-through agreement to protect the commercial value of computer programs and databases is entirely understandable,[67] even if the distinction between tangible property and intangible intellectual property rights, on which the first sale doctrine depends, is a matter of poorly understood copyright law metaphysics when applied in the electronic context.[68] That impulse has been sharpened by the growth both in the number and value of online commercial databases, particularly because American copyright law provides little legal

---

[64] The first sale doctrine in copyright law restrains application of the copyright owner's exclusive right to distribute the copyrighted work. *See* 17 U.S.C. §§ 106(3), 109(a) (2000). Once the owner has distributed a particular copy of the work in a "first sale," the owner has no further legal right to control further disposal of that copy. *See id.* §§ 106(3) (exclusive right to distribute copies of the work), 109(a) (first sale defense).

[65] Madison, *supra* note 56, at 1057–58.

[66] *Id.* at 1058–59.

[67] *See* Lemley, *supra* note 59, at 1242–48; Madison, *supra* note 56, at 1055–76.

[68] *Cf.* McDonald's Corp. v. Shop at Home, Inc., 82 F. Supp. 2d 801, 803–04, 817 (M.D. Tenn. 2000) (refusing to enforce, in context of trademark case, "license" label affixed to bag containing Beanie Baby toys purchased by defendant). *Compare* Softman Prods. Co. v. Adobe Sys., Inc., 171 F. Supp. 2d 1075, 1082–85 (C.D. Cal. 2001) (declining to recognize "license" of tangible copies of copyrighted computer programs), *with* Adobe Sys., Inc. v. Stargate Software Inc., 216 F. Supp. 2d 1051, 1060 (N.D. Cal. 2002) (enforcing software license). The doctrinal confusion that exists in this area is carefully summarized in David Nimmer et al., *The Metamorphosis of Contract into Expand*, 87 CAL. L. REV. 17, 34–41 (1999). The distinction between the tangible and the intangible is also a matter of poorly understood metaphysics in the commercial law context. Proposed revisions to Article 2 of the Uniform Commercial Code would clarify its scope by specifically excluding transactions in "computer information," including such transactions where the only "goods" involved are media on which the "computer information" is encoded. *See* U.C.C. Art. 2 (Proposed Official Draft of Amendments to Article 2—Sales, 2002), *available at* http://www.law.upenn. edu/bll/ulc/ucc2/annual2002.htm.

protection to database owners.[69] Fuzzy lines among software, data, and services online have led to the proliferation of click-through agreements in the service-provider context. The spread of electronic content in all its many contemporary forms and the low cost of presenting users with click-through icons and links means that these agreements have been a relatively straightforward way for providers and producers to establish apparently binding contractual relationships with nearly everyone, regulating access to and use of electronic information.

Because for all the world these "licenses" look like "contracts," whether they are enforceable (as to both commercial terms, such as a

---

[69] Computer programs are copyrightable literary works. *See, e.g.*, 17 U.S.C. §§ 101, 102(a); Fonar Corp. v. Domenick, 105 F.3d 99, 104 (2d Cir. 1997). Computer databases, at least in the absence of some minimal creativity in the selection or arrangement of data, are not. *See* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 362–64 (1991). Since the decision in *Feist*, database producers have sought refuge in a variety of legal strategies. Efforts in Congress to obtain federal legislative protection for databases have been ongoing for some time. Efforts to address the problem via application of the tort of misappropriation, based on the Supreme Court's decision in *International News Service v. Associated Press*, 248 U.S. 215 (1918), have yielded mixed results. *Compare* Nat'l Basketball Ass'n v. Motorola, Inc., 105 F.3d 841, 854 (2d Cir. 1997) (finding that real-time transmission of basketball scores was not misappropriation), *with* Morris Communications Corp. v. PGA Tour, Inc., 117 F. Supp. 2d 1322, 1328–29 (M.D. Fla. 2000) (finding that real-time transmission of golf scores was misappropriation). In Europe, database providers have had more success in restricting access based on unfair competition principles, using sui generis legal protection of electronic databases. *See, e.g.*, British Horseracing Bd. Ltd. v. William Hill Org. Ltd., [2001] R.P.C. 31, 2001 WL 98034 (Eng.) (Ch.), *rev'd* [2002] E.C.D.R. 4, 2001 WL 825162 (Eng.) (C.A.) (interpreting the European Parliament and Council Directive 96/9/EC of 11 March 1996, European Database Directive, 1996 O.J. (L 77) 20. on the Legal Protection of Databases). For discussion of a Danish case, see *EU Database Directive Invoked to Support Order Barring Deep Linking to News Sites*, 7 ELECTRONIC COM. & L. REP. (BNA) 714, 714–15 (July 17, 2002), *Danish Newspapers Win Deep Linking Battle*, EUROPEMEDIA, July 8, 2002, 2002 WL 10691019, and *Deep Link Foes Get Another Win*, WIRED NEWS, July 8, 2002, *at* http://www.wired.com/news/politics/0,1283,53697,00.html (partial translation of opinion *at* http://www.newsbooster.com/?pg=judge&lan=eng) (all reporting on Danish Newspaper Publishers' Ass'n v. Newsbooster.com ApS (Bailiff's Court of Copenhagen, Denmark, July 5, 2002)). For a discussion of a German case, see *Deep Linking Takes Another Blow*, WIRED NEWS, July 25, 2002, *at* http://www.wired.com/news/politics/0,1283,54083,00.html (reporting on Mainpost v. Newsclub (Upper Court Munich, July 2002)). For discussion of a Dutch case, see Armand Killan, *Dutch Supreme Court Decision Broadens Protection of Databases*, 16 WORLD INTELL. PROP. REP. (BNA) No. 6, at 8 (June 2002) and *Supreme Court Bans Unauthorised Deeplinking*, EUROPEMEDIA, Mar. 27, 2002, *at* http://www.europemedia.net/shownews.asp?ArticleID=9666&Print=true (reporting on Netherlands Assoc. of Realtors v. De Telegraaf (Supreme Court of the Netherlands, Mar. 22, 2002)). For a discussion of these and other, similar cases, see P. Bernt Hugenholtz, The New Database Right: Early Case Law from Europe, Presentation at the Ninth Annual Conference on International IP Law and Policy, Fordham University School of Law (Apr. 15–20, 2001), *available at* http://www.ivir.nl/publications/hugenholtz/fordham2001.html.

choice of forum and limitation of remedy, and scope-of-use terms) is a question that has been answered primarily in terms of the law of offer and acceptance, or contract-as-assent, rather than in terms of the legitimacy of restrictions on access to the underlying computer system, service, data, or work. Answering the question in contractual terms is also due largely to the typical presence of terms that address the parties' commercial relationship (limitations of liability and warranty, choice of law, and choice of forum) as well as use of the underlying program, data, or service. Many of the available decisions interpreting shrinkwrap and click-through licenses concern choice-of-forum and warranty issues, areas of law that often bring with them specialized perspectives on contract enforcement, including special solicitude for promoting commercial transactions[70] and private forms of dispute resolution.[71] What started as a regime of access control for computer programs has benefited substantially from presumptions in commercial law that promote shrinkwrap and click-through forms for reasons having nothing to do with access to information.

The commercial law approach has been tempered by courts' increasing recollection of the premise that "it takes two" to make a contract. As the following brief history recounts, although shrinkwrap and click-through law lacks any compelling synthesizing metaphor,[72] it

---

[70] *See generally* Fred H. Miller, *The Uniform Commercial Code: Will the Experiment Continue?*, 43 MERCER L. REV. 799 (1992) (describing success of the UCC in promoting uniformity in commercial practice). Sections 2-204 and 2-207 of the Uniform Commercial Code, which abandon the common-law "mirror image rule" of contract formation via offer and acceptance in favor of a more pragmatic "expression of acceptance" framework, exemplify the phenomenon. *See* U.C.C. §§ 2-204, -207 (2001).

[71] *See* 9 U.S.C. § 2 (2000) (Federal Arbitration Act presumption in favor of enforcement of agreements to arbitrate); Carnival Cruise Lines, Inc. v. Shute, 499 U.S. 585, 589, 597 (1991) (reflecting strong federal policy supporting forum selection clauses); Moses H. Cone Mem'l Hosp. v. Mercury Constr. Corp., 460 U.S. 1, 24 (1983) (referring to liberal federal policy favoring arbitration agreements); Bremen v. Zapata Off-Shore Co., 407 U.S. 1, 8–15 (1972) (also reflecting strong federal policy supporting forum selection clauses). There are many examples of the forum selection clause bias at work in electronic information contexts. *See, e.g.*, Graves v. Pikulski, 115 F. Supp. 2d 931, 934–35 (S.D. Ill. 2000); Decker v. Circus Circus Hotel, 49 F. Supp. 2d 743, 748 (D.N.J. 1999); *cf.* Monsanto Co. v. McFarling, 302 F.3d 1291, 1294, 1296 (Fed. Cir. 2002) (enforcing forum selection clause in printed contract of adhesion governing access to Roundup Ready seed technology). *See generally* Barnett v. Network Solutions, Inc., 38 S.W.3d 200 (Tex. App. 2001).

[72] Shrinkwrap law under the contract-as-assent metaphor has never made much sense to software users because it had nothing to do with how they acquired or used software. *See* Dennis M. Patterson, *Law's Pragmatism: Law as Practice & Narrative*, 76 VA. L. REV. 937, 983–85, 989–95 (1990) (describing problem of standard form contracts as problem of narrative). To the extent that sections 2-204 and 2-207 of the UCC manifest a narrative of "the deal," the deal is signified by the acts of exchanging forms. *See* U.C.C. §§ 2-204, -207. In

has largely evolved to the point of at least formal recognition of the need for user "acknowledgement" of a license or access control offered by an information proprietor. To the extent that courts focus on contract formation issues, the law has worked (precariously) to balance proprietor and user interests.[73]

1. *Step-Saver Data Systems, Inc. v. Wyse Technology*

Three cases serve as landmarks in the evolution of click-through law. The first addressed an authentic boxtop license, printed on the outside of a package that contained a copy of a computer program, and deserves only brief mention.[74] Step-Saver Data Systems, Inc. sold computer systems that included software purchased from The Software Link ("TSL").[75] The systems malfunctioned, and Step-Saver sued TSL for breach of warranty.[76] TSL argued that form language printed on the top of the packaging in which it delivered its software to Step-Saver constituted the complete agreement of the parties, and that with that language TSL had effectively disclaimed any warranties.[77] The U.S. Court of Appeals for the Third Circuit reversed the trial court's ruling in favor of TSL with respect to Step-Saver's warranty

---

practice, specific terms were rarely negotiated, and enforcement was denied only when a particular term exceeded standard commercial expectations. Sending the form, in other words, was more important than what the form said, so long as standard commercial practice was observed. Without two commercial parties, however, the ritual was abstracted and decontextualized into "open the box" (or "click on the icon"), agree to the terms. Without a practice of contracting to which the law attached, no one and no court has articulated any persuasive reason, aside from the internal logic of judicial decisionmaking, to adhere to the contract-as-assent model. *See* Margaret Jane Radin, *Humans, Computers, and Binding Commitment*, 75 IND. L.J. 1125, 1126–28 (1999).

[73] An important sub-theme in these cases is the occasional willingness of courts to accept the enforceability of a click-through or shrinkwrap agreement as given and proceed to analysis of the enforceability of particular contract terms. The recent decision of the U.S. Court of Appeals for the Federal Circuit in *Bowers v. Baystate Techs., Inc.*, 320 F.3d 1317, 1323–27(2003), which held that a "no reverse engineering" clause in a shrinkwrap license for packaged computer software was not preempted by federal copyright law, suffers from precisely this flaw. The court engaged in no analysis whatsoever of the enforceability of the license as a matter of contract law. The court compounded this omission by characterizing the commercial transaction as a "sale." *See id.* at 1322. If the software were in fact "sold," then there was no license, and the "no reverse engineering" clause would clearly be preempted under the "first sale doctrine."

[74] Step-Saver Data Sys., Inc. v. Wyse Tech., 939 F.2d 91, 96 (3d Cir. 1991).

[75] *Id.* at 93.

[76] *Id.* at 94.

[77] *Id.* at 94–95.

claims.[78] In effect, the court of appeals held that the boxtop license was not enforceable.[79]

The details of the court's analysis are relatively unimportant here, but certain of its premises have had lasting impact. First, the court accepted the parties' agreement that the terminals and the program were "goods" within the meaning of Article 2 of the Uniform Commercial Code ("UCC"),[80] and it therefore analyzed the legal effect of the parties' offer-and-acceptance correspondence under the rules of section 2–207 of that Article.[81] Second, given the sequence of the parties' order and shipment correspondence, the court concluded that TSL's warranty limitation did not become part of the parties' agreement because it was proposed, via boxtop license, after the commercial agreement had been reached.[82] Each package of the software delivered by TSL had printed on its top a "license" that purported to disclaim all relevant warranties, that limited the purchaser to a return-and-replace remedy, and that stated that acceptance of the terms of the license occurred when the box was opened.[83] The warranty limitation represented a "material alteration" to the contract already formed. Implicitly, but never explicitly, the court concluded that Step-Saver had not "accepted" or assented to this new term merely by opening the box.[84]

---

[78] *Id.* at 108.

[79] *See Step-Saver*, 939 F.2d at 108.

[80] The court noted that the parties did not contest the application of Article 2 to their dispute. *See id.* at 94 n.6. The court did offer a supporting citation to *Advent Systems Ltd. v. Unisys Corp.*, 925 F.2d 670, 674–76 (3d Cir. 1991), in which the court thoughtfully analyzed whether Article 2 applies to transactions in computer software. The *Step-Saver* court's willingness to accept the application of Article 2 was based in part on the underlying policy of the UCC to promote the expansion of commercial practices, and in part on the premise that computer software is necessarily embodied in tangible media, or goods.

[81] Section 2-207 of the UCC sets out a statutory alternative to the common law "battle of the forms." Under this section, a binding contract may be found notwithstanding conflict between forms exchanged between buyer and seller. U.C.C. § 2-207 (2001). Terms that do not match may be included in the parties' agreement so long as they do not conflict with the parties' commercially reasonable expectations or if they are separately assented to. *Id.*

[82] *Step-Saver*, 939 F.2d at 103.

[83] *Id.* at 96–97.

[84] *Id.* at 105–06. Two post-*Step-Saver* courts also refused to enforce boxtop agreements, although on different grounds. *See* Vault Corp. v. Quaid Software, Ltd., 847 F.2d 255, 258–59 (5th Cir. 1988) (holding enforceability of shrinkwrap agreement preempted under federal copyright law); Ariz. Retail Sys. v. The Software Link, Inc., 831 F. Supp. 759, 764 (D. Ariz. 1993) (license terms excluded from the parties' agreement under section 2-209 of the UCC). *Arizona Retail Systems* did allow for the possibility that under section 2-207, if the software developer's "offer" consisted of delivery of shrinkwrapped software to the user,

Both the court's use of Article 2 and its focus on the assent issue sowed the seeds of later problems. Application of Article 2 was not contested by the parties or analyzed by the court.[85] Rather than closing the door on the question of shrinkwrap enforcement, *Step-Saver* in effect offered an invitation, within the contract-as-assent model, that later information proprietors and courts were happy to accept. Largely because the Third Circuit applied Article 2 to this computer software transaction, Article 2 has become the de facto legal standard governing cases not only of defective software, but also of software licensing generally.[86]

2. *ProCD, Inc. v. Zeidenberg*

Starting from the same Article 2 premise, *ProCD, Inc. v. Zeidenberg* dramatically altered the landscape roughed out by *Step-Saver,* in effect reversing what had appeared to be a presumption against shrinkwrap enforceability and installing in its place a presumption favoring the validity of shrinkwrap and click-through agreements and their cog-

---

opening the shrinkwrapped package could amount to "acceptance" of the license within. *See also* U.S. Surgical Corp. v. Orris, Inc., 5 F. Supp. 2d 1201, 1206 (D. Kan. 1998), *aff'd per curiam*, 185 F.3d 885 (Fed. Cir. 1999) (relying on *Step-Saver* to invalidate "single use" notice restriction affixed to label for patented surgical instruments purchased by defendant).

[85] *Step-Saver*, 939 F.2d at 95 n.6. Computer software is not a "good" as that term historically has been used in commercial law. There are good reasons to conclude that commercial practice involving transfers of software did not then and does not now recognize a computer program as the commercial equivalent of a widget. This, of course, is one of the leading arguments behind development and adoption of UCITA. *See supra* note 54; *see also* I.Lan Sys., Inc. v. Netscout Serv. Level Corp., 183 F. Supp. 2d 328, 332 (D. Mass. 2002) (noting "void" in commercial law regarding regulation of software transactions); Mary Jo Dively, *The Use of Standard Form Contracts in the Information Industry*, *in* UNDERSTANDING ELECTRONIC CONTRACTING: THE IMPACT OF REGULATIONS, NEW LAWS & NEW AGREEMENTS, at 573, 582–90 (PLI Patents, Trademarks, Copyrights, and Literary Property Course, Handbook Series No. 697, 2002) (providing a practitioner's view of the need for UCITA). Article 2 was specifically designed to make the process of forming an agreement less subject to common-law formalities, and less subject to hijacking by a party that manipulated the sending and receipt of purchase forms in such a way as to effectively impose its terms on the other party. In practice, shrinkwrap and click-through agreements are alleged to have precisely that effect. *See* Jean Braucher, *Delayed Disclosure in Consumer E-Commerce as an Unfair and Deceptive Practice*, 46 WAYNE L. REV. 1805, 1806–08 (2000).

[86] *See* Diana G. Richard & Michael K. Murphy, *Frequently Litigated Computer Software Contract Clauses: Contract Drafting Advice for the Computer Lawyer*, *in* INFORMATION TECHNOLOGY LITIGATION, REPRESENTING YOUR CLIENT IN SOFTWARE PERFORMANCE & SYSTEM FAILURE CLAIMS, at 33, 62–64 (PLI Patents, Trademarks, Copyrights, and Literary Property Course, Handbook Series No. 700, 2002). *See generally* Lorin Brennan, *Why Article 2 Cannot Apply to Software Transactions*, 38 DUQ. L. REV. 459 (2000); Andrew Rodau, *Computer Software: Does Article 2 of the Uniform Commercial Code Apply?*, 35 EMORY L.J. 853 (1986).

nates.[87] Judge Easterbrook's opinion in *ProCD* addressed precisely the question left open by *Step-Saver*, the effect of the purchaser's (or licensee's) conduct in the face of notice, on the product itself, that such conduct constituted acceptance of a license or other agreement.[88] Matthew Zeidenberg purchased three packages of ProCD's SelectPhone database and search engine, distributed on CD-ROM discs and packaged with a license agreement that prohibited purchasers of the discs from distributing their contents and from making them available in any networked environment.[89] The outside of the packaging included a small notice that an agreement was included within, but the package did not otherwise include its terms.[90] The terms were spelled out in the user guide that accompanied the discs and were referred to on fields on the computer screen when the user used the SelectPhone CD-ROMs.[91] When ProCD sued Zeidenberg for breach of the license agreement (Zeidenberg having uploaded the contents of the SelectPhone database to an Internet site), Zeidenberg argued that he was not bound by those terms.[92] Reviewing the claim under three different sections of Article 2 of the UCC—sections 2–206, 2–207, and 2–209—the district court held that whatever agreement Zeidenberg and ProCD had entered into did not include the terms of the license.[93]

The U.S. Court of Appeals for the Seventh Circuit reversed, holding that ProCD was entitled to prevail on its contract claim.[94] Its resolution of the shrinkwrap issue in favor of enforceability was unequivocal, although the specifics of its rationale are hazy.[95] As in *Step-Saver*, the court in *ProCD* assumed that Article 2 of the UCC governed the

---

[87] *See* ProCD, Inc., v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996); *Step-Saver*, 939 F.2d at 105–06. From a common-law perspective, the case has had an impact that is dramatically out of step with the actual holding of the court. The parties in *ProCD* were before the court under diversity jurisdiction, and the court actually ruled that a Wisconsin court, were it to decide the case, would enforce the agreement in question under Wisconsin's version of Article 2 of the UCC. 86 F.3d at 1453. No Wisconsin court had decided a shrinkwrap case at the time that *ProCD* was decided, and no Wisconsin court has decided such a case, even today.

[88] *ProCD*, 86 F.3d at 1450–51.

[89] *Id.* at 1450.

[90] *Id.*

[91] *Id.*

[92] *Id.*

[93] *See* ProCD, Inc. v. Zeidenberg, 908 F. Supp. 640, 651–55 (W.D. Wis. 1996).

[94] *ProCD*, 86 F.3d at 1450.

[95] *See id.* at 1455.

transaction.[96] Because in this merchant/consumer transaction there was no battle-of-forms to contend with, the court relied on section 2–204 of the UCC, an all-purpose contract formation section that, by design, discards traditional, formal common-law standards for contract formation.[97] Thus unencumbered by common-law notions of "offer" and "acceptance," the court nonetheless proceeded to analyze the transaction using a formal, common-law-style contract-as-assent model, though without the sensitivity to context that typically characterizes common-law analysis.[98] The court focused in part on the shrinkwrap transaction, in that the product package included a small notice referring to license terms inside the package.[99] The terms of Zeidenberg's purchase therefore provided at least constructive knowledge of the existence of additional terms, and acceptance of those terms, at the time that he bought the software.[100] In part, the court also focused on the click-through dimension of the transaction, asserting that Zeidenberg's assent to ProCD's license terms occurred when he actually used the software and accessed SelectPhone data.[101] The court did not carefully distinguish between the two interpretations.[102]

---

[96] *See id.* at 1452–53.

[97] *Id.* at 1452. The relevant text of section 2-204 provides: "A contract for the sale of goods may be made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of such a contract." U.C.C. § 2-204(1) (2001).

[98] *See ProCD*, 86 F.3d at 1452–53.

[99] *See id.* at 1450–51.

[100] *See id.* at 1452.

[101] *See id.* at 1450. The exterior of the package Zeidenberg purchased informed purchasers of the existence of a license agreement inside. *Id.* The printed license agreement inside informed purchasers that using the computer program and the data constituted acceptance of the restrictions on use stated in the printed materials and on the computer screen. *Id.* It is not clear, therefore, whether the offer/acceptance sequence took place at the point-of-sale, or at the point-of-computer-mouse, or both.

[102] *See id.* at 1450–51. The Seventh Circuit extended the analysis in *ProCD* to non-electronic agreements for sales of goods in *Hill v. Gateway 2000, Inc.*, 105 F.3d 1147, 1148–50 (7th Cir. 1997) (holding customers bound by agreement with computer manufacturer where notice inside box asserted that terms would be deemed accepted if the computer were not returned within thirty days), in a manner that suggests that the *ProCD* decision was grounded primarily on Zeidenberg's purchase of the product with knowledge that additional contract terms were forthcoming. *See also I.Lan Sys.*, 183 F. Supp. 2d at 338 (illustrating same rationale, applied to a limitation of liability clause in click-through license of software sold pursuant to value added reseller agreement). Other courts interpreting *ProCD* have taken special notice of the court's statement that Zeidenberg could not use the SelectPhone software without specifically assenting to the license when it appeared on his screen. *See ProCD*, 86 F.3d at 1450; Specht v. Netscape Communications Corp., 150 F. Supp. 2d 585, 592 (S.D.N.Y. 2001), *aff'd*, 306 F.3d 17 (2d Cir. 2002).

As an application of the commerce-promoting policies of the UCC, *ProCD* appears uncontroversial, particularly if the case is understood as depending on Zeidenberg's actual advance knowledge of restrictions that accompanied his purchase of an actual box containing SelectPhone CD-ROMs.[103] Given the court's reliance on a formal contract-as-assent metaphor, as information access policy the case has more disturbing implications.[104] Whatever the merits of Article 2's relaxed approach to contract formation issues, the notion of assent (even in the context of doctrines of "material alteration" under section 2–207) has little resonance in an information environment where consumers have little or no background expectations against which to measure their "assent" experience.[105] Worse, there is little reason to think that the case should be read restrictively as based on Zeidenberg's actual notice of ProCD's terms. With respect to entirely electronic transactions, *ProCD*, or its Seventh Circuit progeny, have been cited repeatedly by other courts as authority for the propositions that choice of forum, limitation of remedy, *and contractual restrictions on access and reuse* are enforceable so long as the user undertakes some conscious act that can be deemed to ratify terms supplied by the proprietor, even if the user's knowledge of the terms comes after the act of ratification.[106] It is contract-as-assent, writ large.

---

[103] *See* Robert A. Hillman & Jeffrey J. Rachlinski, *Standard-Form Contracting in the Electronic Age*, 77 N.Y.U. L. REV. 429, 487–88 (2002) (noting consistency of *ProCD* with Article 2's "blanket assent" presumption, coupled with the doctrine of reasonable expectations). Even on this assumption, as a matter of contract law the case is not unproblematic. Zeidenberg himself may well have known of the license restriction, but it is far from clear that a typical or reasonable acquirer of the SelectPhone product, or of an equivalent electronic information product, would be equally cognizant of the license "offer." Also, as a matter of copyright law, the court's summary rejection of the argument that restrictions on Zeidenberg's reuse of the telephone number data were preempted by federal law remains controversial. *See* Brief of Amici Curiae in Support of Petition for Panel Rehearing and Rehearing En Banc at 8–9, Bowers v. Baystate Techns., Inc., 320 F.3d 1317(Fed. Cir. 2003), *available at* http://jurist.law.pitt.edu/amicus/bowers_v_baystate_rehearing.pdf.

[104] *See ProCD*, 86 F.3d at 1452–53.

[105] *See* Madison, *supra* note 56, at 1055–58.

[106] *See, e.g.*, *Bowers*, 320 F.3d at 1324–25; Lozano v. AT&T Wireless, 216 F. Supp. 2d 1071, 1073 (C.D. Cal. 2002) (acceptance of printed terms analyzed under *ProCD*); *Adobe Sys.*, 216 F. Supp. 2d at 1051; Bischoff v. DirecTV, Inc., 180 F. Supp. 2d 1097, 1104–05 (C.D. Cal. 2002) (acceptance of printed terms analyzed under *ProCD* and *Hill*); 1-A Equip. Co. v. ICode, Inc., 43 U.C.C. Rep. Serv. 2d (CBC) 807, No. 0057CV467, 2000 WL 33281687, at *2–3 (D. Mass. Nov. 17, 2000), *appeal dismissed*, 2003 Mass. App. Div. 30; O'Quin v. Verizon Wireless, No. CIV.A.01-855-D, 2003 WL 1889293, at *4–5 (M.D. La. Feb. 7, 2003); *Register.com*, 126 F. Supp. 2d at 245–46; Scott v. Bell Atlantic Corp., 726 N.Y.S.2d 60, 64 (App. Div. 2001), *aff'd as modified by* Goshen v. Mutual Life Ins. Co. of N.Y., 774 N.E.2d 1190 (N.Y. 2002); Madison, *supra* note 56, at 1053. Where access to information is not involved,

3. *Specht v. Netscape Communications Corp.*[107]

With the ebbing of the dot.com economy, the high tide of click-through enforceability represented by *ProCD* may dissipate somewhat as well.[108] Yet contract-as-assent remains the dominant metaphor.[109] In *Specht v. Netscape Communications Corp.*, the U.S. Court of Appeals for the Second Circuit declined to enforce a click-through agreement offered on the Internet in connection with downloading a computer program.[110] The court's analysis leaves ample room for enforcement

---

equivalent arguments have not been accepted uniformly. *Compare* Boomer v. AT&T Corp., 309 F.3d 404, 415 (7th Cir. 2002) (enforcing arbitration clause in customer service agreement with long distance carrier, given use of services after mailed notice of offer, citing *Hill*), Cook's Pest Control, Inc. v. Rebar, No. 1010897, 2002 WL 31780946, at *5 (Ala. Dec. 13, 2002) (enforcing terms of disclaimer of arbitration agreement proposed by company, where customer returned service contract with payment and addendum proposing modified terms, and company accepted by negotiating check and continuing service), *and* Southtrust Bank v. Williams, 775 So. 2d 184, 190–91 (Ala. 2000) (enforcing notice of change to arbitration agreement regarding bank account), *with* Mattingly v. Hughes Elec. Corp., 810 A.2d 498, 505–09 (Md. Ct. Spec. App. 2002) (finding arbitration clause allegedly barring class action by satellite TV subscriber invalid despite alleged "constructive acceptance" by customer's continued use of service after receipt of modified terms in the mail, distinguishing *ProCD* and *Hill*), *and* Badie v. Bank of Am., 79 Cal. Rptr. 2d 273, 291 (Ct. App. 1998) (refusing to enforce notice of change unilaterally imposed by bank, despite customer's prior assent to form agreement permitting bank to change terms).

[107] 306 F.3d 17 (2d Cir. 2002). The district court opinion, which used slightly different reasoning, is reported in 150 F. Supp. 2d 585 (S.D.N.Y. 2001).

[108] *See* Comb v. Paypal, Inc., 218 F. Supp. 2d 1165, 1175, 1177 (N.D. Cal. 2002) (declining to enforce click-through agreement to arbitrate on grounds of both procedural and substantive unconscionability); *Adobe Sys.*, 171 F. Supp. 2d at 1080, 1083, 1087, 1093 (C.D. Cal. 2001) (refusing to enforce software "license" where reseller of software argued that plaintiff's claims were limited under first sale doctrine, and where reseller never installed software and therefore never assented to click-through license barring unauthorized access).

[109] *See Bowers*, 320 F.3d at 1323–25 (assuming but not deciding that a shrinkwrap agreement is enforceable as a matter of contract law); DeJohn v. The .TV Corp. Int'l, 245 F. Supp. 2d 913, 915–17 (N.D. Ill. 2003) (enforcing forum selection clause where customer was required to click on box indicating assent); *Adobe Sys.*, 216 F. Supp. 2d at 1060 (concluding that software developer can enforce shrinkwrap agreement's characterization of transaction with customer as "license" rather than "sale"); Hughes v. McMenamon, 204 F. Supp. 2d 178, 181 (D. Mass. 2002) (enforcing forum selection clause in America Online Terms of Service Contract where subscriber clicked on terms when he became subscriber); *I.Lan Sys.*, 183 F. Supp. 2d at 338–39 (enforcing click-through license under authority of Article 2 and *ProCD*, where defendant had previously installed plaintiff's software and therefore had reason to expect existence of license); Forrest v. Verizon Communications, Inc., 805 A.2d 1007, 1010, 1015 (D.C. 2002) (enforcing click-through forum selection clause); Moore v. Microsoft Corp., 741 N.Y.S.2d 91, 92 (App. Div. 2002) (enforcing click-through agreement under *ProCD* on the ground that the consumer downloaded the software and used it with knowledge of the existence of a license).

[110] 306 F.3d 17, 20 (2d Cir. 2002).

of more carefully crafted agreements, but its approach suggests some increasing recognition of user interests in contract formation, even under the prevailing contract-as-assent paradigm.[111]

The plaintiffs in *Specht* raised substantive claims under the federal Electronic Communications Privacy Act and the CFAA in connection with alleged surveillance of their activities, as users, while using Netscape's SmartDownload software on the Internet.[112] Netscape argued that a license that accompanied the SmartDownload product contained an enforceable agreement to arbitrate all disputes.[113] Netscape moved to stay the federal court proceedings in favor of private arbitration.[114]

The district court denied Netscape's motion, and the Second Circuit affirmed, concluding that the plaintiffs had not given their assent to the license agreement offered by Netscape.[115] In so doing, the Second Circuit was careful to tie its ruling to the manner in which Netscape's alleged contract offer was presented to Internet users.[116] SmartDownload was, for most of the plaintiffs, a product available for download for free from Netscape's Web site.[117] Users were able to download the program from Netscape's site simply by clicking on a "Download" icon.[118] At the bottom of that download page, Netscape had included text inviting, but not requiring, users downloading the software to review a licensing agreement before downloading and using the software.[119] The agreement itself was not available on the download page but was instead accessible only through a series of hyperlinks.[120] The court found that it could not be reasonably concluded that those who downloaded Netscape's program could be deemed to have manifested assent to the proposed terms, because it could not be concluded that those users had actual or constructive notice of those terms.[121]

---

[111] *See id.* at 21–25.

[112] *Id.* at 21.

[113] *Id.* at 21–22.

[114] *Id.* at 20.

[115] *Specht*, 306 F.3d at 20–21.

[116] *See id.* at 20.

[117] *Id.* One plaintiff apparently downloaded the program from a shareware site. This fact did not change the court's conclusion. *Id.* at 24.

[118] *Id.* at 22.

[119] *Id.* at 23–24.

[120] *See Specht*, 306 F.3d at 29–30. The first hyperlink took the user to an index of hyperlinked license agreements; the user was then expected to select the appropriate license agreement and to read its text, via a second hyperlink.

[121] *See id.* at 28–30.

The Second Circuit relied on both common law and UCC Article 2 "assent" principles to analyze the question of contract formation.[122] The court concluded that the act of downloading the software did not unambiguously manifest assent to Netscape's license terms.[123] Largely because of the location and format of the notice of proposed terms, the user was not made aware that downloading the software was an act of any significance with respect to any contract.[124] "A consumer's clicking on a download button does not communicate assent to contractual terms if the offer did not make clear to the consumer that clicking on the download button would signify assent to those terms."[125] "Plaintiffs were responding to an offer that did not carry an immediately visible notice of the existence of license terms or require unambiguous manifestation of assent to those terms. Thus, plaintiffs' 'apparent manifestation of . . . consent' was to terms 'contained in a document whose contractual nature [was] not obvious.'"[126] The court distinguished this case from situations (such as those used by Netscape for other computer programs available on the Internet) in which the user was required to click on an "accept" or "acknowledge" icon before being permitted to access the relevant data, service, or program.[127]

4. Click-Through Agreements, Context, and Places on the Net

As a practical matter, *Specht* seems clearly preferable to *ProCD* from the standpoint of the consumer, whether goods or information is involved.[128] The Article 2-based evolution of shrinkwrap law for access control comes at a fairly steep price, however coherent doctrinally the evolution may be. The initial rationale for applying Article 2 to these cases was that computer programs were delivered via media (and in packages) that were essentially akin to goods, even if they were not "classic" goods.[129] Applying the framework of Article 2 therefore made sense. There were merchants. They were treating copies of computer programs essentially as they would have treated equivalent

---

[122] *See id.*

[123] *Id.* at 30.

[124] *Id.* at 29–30.

[125] *Specht*, 306 F.3d at 29–30.

[126] *Id.* at 31 (quoting Windsor Mills, Inc. v. Collins & Aikman Corp., 101 Cal. Rptr. 347, 351 (Ct. App. 1972)). The case was decided under California law.

[127] *See id.* at 31–32.

[128] *See Specht*, 306 F.3d at 17; *ProCD*, 86 F.3d at 1447.

[129] *See Specht*, 306 F.3d at 28; *ProCD*, 86 F.3d at 1452.

widgets.[130] There was the "battle of the forms" that Article 2 largely eradicated, because Article 2 embodied the notion that common-law formalities could be discarded in the face of virtually universal and widely understood everyday practices and expectations.[131] There was, in sum, a coherent commercial context in which application of Article 2 could be justified, and in which, in principle, assent was assumed (via context) as often as it actually was proved.[132]

If *Specht* fairly represents the present equilibrium in click-through law,[133] the formal contract-as-assent metaphor may not be enough to

---

[130] *See Specht*, 306 F.3d at 28; *ProCD*, 86 F.3d at 1452.

[131] *See* U.C.C. Art. 2 (2001); Rodau, *supra* note 86, at 857–58.

[132] *See generally* Rodau, *supra* note 86, at 864–910, for an argument justifying application of Article 2 to software licenses on essentially these grounds.

[133] *But see supra* note 109 and cases cited therein. For present purposes, I take the most optimistic view of *Specht*, which is that the case is not only well-reasoned but strongly suggestive of the likely evolution of commercial doctrine. *See also* Kunz et al., *supra* note 7, at 306, 411–15. The authors describe the recommendations of a working group on electronic commerce sponsored by the American Bar Association. The working group, taking *Specht* as the most recent case on point, offered recommendations for drafting enforceable click-through agreements. The cases relied on by the working group are: *America Online, Inc. v. Booker*, 781 So. 2d 423 (Fla. Dist. Ct. App. 2001); *America Online, Inc. v. Superior Court*, 108 Cal. Rptr. 2d 699 (Ct. App. 2001); *Caspi v. Microsoft Network, L.L.C.*, 732 A.2d 528 (N.J. Super. Ct. App. Div. 1999); *Celmins v. America Online, Inc.*, 748 So. 2d 1041 (Fla. Ct. App. 1999); *CompuServe, Inc. v. Patterson*, 89 F.3d 1257 (6th Cir. 1996); *Groff v. America Online, Inc.*, No. PC 97-0331, 1998 WL 307001 (R.I. Super. Ct. May 27, 1998); *Hotmail Corp. v. Van$ Money Pie, Inc.*, No. C-98 JW PVTENE, C 98-20064, 1998 WL 388389, 47 U.S.P.Q.2d (BNA) 1020 (N.D. Cal. Apr. 16, 1998); *Lieschke v. RealNetworks, Inc.*, No. 99 C7294, 99 C 7380, 2000 WL 198424 (N.D. Ill. Feb. 11, 2000); *Pollstar v. Gigamania Ltd.*, 170 F. Supp. 2d 974 (E.D. Cal. 2000); *In re RealNetworks, Inc.*, No. 00 C 1366, 2000 WL 631341 (N.D. Ill. May 8, 2000); *Rudder v. Microsoft Corp.*, 2 C.P.R. (4th) 474, No. 97-CT-046534CP, 1999 CarswellOnt 3195 (Westlaw) (Ont. Super. Ct. Justice Oct. 8, 1999); *Specht*, 150 F. Supp. 2d 585; *Scott*, 726 N.Y.S. 2d 60; *Ticketmaster Corp. v. Tickets.com*, No. CV 99-7654, 2000 WL 525390, U.S.P.Q.2d (BNA) 1344 (C.D. Cal. Mar. 27, 2000); *Williams v. America Online, Inc.*, No. 00-0962, 2001 WL 135825, 43 U.C.C. Rep. Serv. 2d (CBC) 1101 (Mass. Super. Ct. Feb. 8, 2001). Kunz et al., *supra* note 7, at 425. The Article does not include *ProCD* itself, although that case was decided only a month before *CompuServe*. It omits cases that address the enforceability of shrinkwrap licenses. *See* Peerless Wall & Window Coverings, Inc. v. Synchronics, Inc., 85 F. Supp. 2d 519, 528–30 (W.D. Pa. 2000), *aff'd*, 234 F.3d 1265 (3d Cir. 2000); Mgmt. Computer Controls, Inc. v. Charles Perry Constr., Inc., 743 So. 2d 627, 631–32 (Fla. App. 1999) (upholding shrinkwrap license); M.A. Mortenson Co., v. Timberline Software Corp., 998 P.2d 305, 314 (Wash. 2000) (same). Also omitted are the so-called "Gateway cases," in which courts address the validity of assent obtained via a customer's keeping a computer shipped by mail beyond a number of days designated by the seller. *See Hill*, 105 F.3d at 1149–50 (finding assent); Klocek v. Gateway, Inc., 104 F. Supp. 2d 1332, 1139–42 (D. Kan. 2000) (finding no assent); Westendorf v. Gateway 2000, Inc., No. 16913, 2000 WL 307369, 41 U.C.C. Rep. Serv. 2d (CBC) 1110 (Del. Ch. Mar. 16, 2000), *aff'd*, 763 A.2d 92 (Del. 2000) (finding assent); Brower v. Gateway 2000, Inc., 676 N.Y.S.2d 569, 571–72 (App. Div. 1998) (same); Licitra v. Gateway, Inc., 734 N.Y.S.2d 389, 391–93 (Civ. Ct. 2001) (finding no assent). A number of other courts have addressed the legal effects of standard

sustain it.[134] The context described in the last paragraph no longer exists with respect to many, if not most, of the circumstances in which click-through and related agreements, and particularly access-limiting provisions, are intended to be enforced.[135] Although courts are starting to realize that *mutual* assent may actually mean something more than "typical user expectations," it is equally clear that neither user assent nor those expectations have any consistent meaning on which courts, or the parties before them, may rely.[136] Courts may increas-

---

form notices in the computer software and/or Internet context. *See, e.g.*, Green v. Am. Online (AOL), 318 F.3d 465, 472 (3d Cir. 2003) (holding AOL immune from suit for defamation based on content posted by third party; ruling based in part on terms of AOL Member Agreement between AOL and plaintiff); Kilgallen v. Network Solutions, Inc., 99 F. Supp. 2d 125, 128–29 (D. Mass. 2000) (enforcing terms in electronic notice of Web site registration); Am. Eyewear, Inc. v. Peeper's Sunglasses & Accessories, Inc., 106 F. Supp. 2d 895, 900–01 (N.D. Tex. 2000) (noting that defendant could have avoided finding of personal jurisdiction based on Internet contacts by using click-through agreement on Web site); Kaczmarek v. Microsoft Corp., 39 F. Supp. 2d 974, 977–78 (N.D. Ill. 1999) (finding claim for breach of warranty barred by warranty contained in software manual that became enforceable when user retained software for specified period of time); Green Book Int'l Corp. v. Inunity Corp., 2 F. Supp. 2d 112, 115 (D. Mass 1998) (noting general acceptance of shrinkwrap agreements); Storm Impact, Inc. v. Software of the Month Club, 13 F. Supp. 2d 782, 790–91 (N.D. Ill. 1998) (interpreting use limitations in shareware license to restrict fair use of program); Novell, Inc. v. Network Trade Ctr., Inc., 25 F. Supp. 2d 1218, 1228–31 (D. Utah 1997) (refusing to enforce shrinkwrap license because of conflict with first sale doctrine in copyright law), *vacated in part on other grounds*, 187 F.R.D. 657 (D. Utah 1999); Microstar v. Formgen, Inc., 942 F. Supp. 1312, 1317–18 (S.D. Cal. 1996), *aff'd in part, rev'd in part*, 153 F.3d 1107 (9th Cir. 1998) (relying on shareware license in part to limit scope of users' rights to create new versions of computer game).

[134] From this point, some contracts scholars conclude that the Article 2 framework remains essentially viable. *See* Hillman & Rachlinski, *supra* note 103, at 475–86 (arguing that existing Article 2 assent framework provides sufficient structure to regulate electronic transactions); James J. White, *Autistic Contracts*, 45 WAYNE L. REV. 1693, 1721–31 (2000) (endorsing "reasonable opportunity to review" standard for enforcement of electronic form agreements).

[135] It is implicit in the discussion above and in application of the assent paradigm that click-through law does not distinguish between access to and use of information delivered on physical media, on the one hand, and access to and use of information delivered entirely electronically, on the other. It does not distinguish between agreements among merchants and agreements involving a merchant and a consumer. It does not distinguish between terms regulating remedy and terms regulating access and use. Legally speaking, shrinkwrap is to be analyzed like click-through is to be analyzed like "browse-wrap." Software producers recognized early on that the tangible-goods based Article 2 model would not last long. The project to draft what became proposed Article 2B of the UCC, now substantially revised and proposed as the UCITA, began in 1992. *See* J.H. Reichman & Jonathan A. Franklin, *Privately Legislated Intellectual Property Rights: Reconciling Freedom of Contract with Public Good Uses of Information*, 147 U. PA. L. REV. 875, 880 (1999) (critiquing proposed Article 2B while sympathetic to interest in abandoning the mutual assent model); *see also supra* note 54.

[136] *See* Reichman & Franklin, *supra* note 135, at 933–36.

ingly require that information proprietors show that information users actually knew what they were doing. With respect to access regulation in the abstract, information users frequently do not know what they are doing. Contract-as-assent is a fiction in the electronic environment, even when it favors consumers.[137]

Information proprietors are searching for more durable alternatives.[138] Before the evolution of the commercial Internet, few alternatives were available. Information proprietors tried revisions to copyright law, and refinements of commercial law, and sometimes both at once.[139] The Internet also allows for framing the issues accounted for by click-through law in a different way, one based on an Internet-as-place metaphor that is far more intuitively comfortable to most Internet users than contract-as-assent. Courts have been increasingly receptive to information proprietors' arguments. Literally, the law, along with the Internet, has taken "shape." Decontextualized assent has been recontextualized as access to places on the Net. "Access to in-

---

[137] Witness the ongoing pitched battle over adoption of UCITA, heavily supported by software developers and opposed by a coalition of consumer groups and (increasingly) corporate and institutional software users. *Compare* UCITA Yes, *at* http://www.ucitayes.org (last visited Jan. 11, 2003) (pro-UCITA coalition of technology companies called the Digital Commerce Coalition), *with* AFFECT, *at* http://www.4cite.org (last visited Nov. 15, 2002) (anti-UCITA coalition named Americans for Fair Electronic Commerce Transactions). An example of the confusing intersection between consumer protection regulation and assent-oriented click-through law is provided by the recent decision in *State ex rel. Stovall v. DVM Enterprises, Inc.*, 62 P.3d 653 (Kan. 2003). The State of Kansas sued an online pharmacy for dispensing controlled substances over the Internet in unconscionable fashion, in violation of the state's consumer protection statute. *Id.* at 654. In support of its unconscionability argument, the state focused on the waiver of liability to which buyers were required to "agree" before purchasing. *Id.* at 656, 659. The court ruled that the defendants' practices were not unconscionable, because the waiver (which the court implicitly accepted as enforceable) concerned a waiver of liability, not of implied warranties of fitness of merchantability, and the products that the buyers (agents for the state, investigating the case) received were not defective. *Id.* at 659–61. The buyers, in short, received precisely what they agreed to receive (limitation of liability included), even though at the time they were required to waive their rights, they could not have known whether that would be so.

[138] *See infra* note 139 and accompanying text.

[139] Article 2B, now UCITA, being the proposed revision of commercial law. *See supra* note 54. Promotion of an extreme view of computing technology that holds that all computer activity involves making numerous "copies" of copyrighted works, each of which has to be authorized by the copyright owner, being the most notorious example of (successful) revision of copyright law. *See* Triad Sys. Corp. v. Southeastern Exp. Co., 64 F.3d 1330, 1335 (9th Cir. 1995); MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 517–18 (9th Cir. 1993). Digital rights management, technology that permits information proprietors to implement fine-grained access contract via software, was developed to bridge the two perspectives. *See* Tom W. Bell, *Fair Use v. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine*, 76 N.C. L. REV. 557, 564–67 (1998).

formation" (the key issue in click-through agreements) has become "access to the information proprietor's physical resources." Contract, where *mutual* assent is necessary, becomes property, where the owner's right to exclude is presumed. The following three Parts explain how the metaphors have been manifested in both common-law and statutory form, via application to commercial problems of diverse but specifically noncommercial legal doctrines.

B. *Trespass to Chattels*

The most blunt of these developments has been the adaptation to the Internet of the ancient doctrine of trespass to chattels,[140] defined in the *Restatement (Second) of Torts* as intentionally "using or intermeddling with a chattel in the possession of another," or "dispossessing another of the chattel."[141] In the electronic information context, the core concept behind the law of trespass is unauthorized use of a computer system connected to a computer network.[142] In the electronic network environment, the concept was used initially to prevent unwanted information from being delivered to the network, a goal that has little to do with traditional notions of regulation of commercial activity between buyers and sellers, or among competitors.[143] More recently, and as adapted for commercial purposes, tres-

---

[140] *See generally* I. Trotter Hardy, *The Ancient Doctrine of Trespass to Websites*, 1996 J. ONLINE L. art. 7 (Oct. 6), *at* http://www.wm.edu/law/publications/jol/95_96/hardy.html.

[141] RESTATEMENT (SECOND) OF TORTS § 217 (1965). Also, in section 265, the *Restatement* provides: "One who uses a chattel with the consent of another is subject to liability in trespass for any harm to the chattel which is caused by or occurs in the course of any use exceeding the consent, even though such use is not a conversion." The Comments to section 217 note both the significance of the requirement that the trespass be intentional and the character of the conduct that, in this context, may be deemed to be intentional:

> The intention required to make an actor liable for trespass to a chattel is similar to that necessary to make one liable for an invasion of another's interest in bodily security, in freedom from an offensive contact, or confinement. . . . Such an intention is present when an act is done for the purpose of using or otherwise intermeddling with a chattel or with knowledge that such an intermeddling will, to a substantial certainty, result from the act. It is not necessary that the actor should know or have reason to know that such intermeddling is a violation of the possessory rights of another.

Id. § 217 cmt. c.

[142] *See* Hardy, *supra* note 140, ¶¶ 1–6.

[143] Given the potential scope of trespass to chattels as a theory of protecting electronic information, it is noteworthy that recent interest in the doctrine arose primarily to protect computers from invasion by unwanted signals (and/or unwanted content) from the outside. Courts, commentators, and legislatures have wrestled at length with economic, temporal, and psychic damage caused to Internet service providers and their customers by

pass to chattels is deployed to prevent unauthorized access to information already present on the network.[144] Several recent courts have awarded injunctive relief to plaintiffs on a theory that electronically accessing the plaintiff's computer network and/or servers, to obtain information without the plaintiff's consent, was unlawful.[145]

For example, in *eBay, Inc. v. Bidders' Edge, Inc.*, the auction Web site eBay sued an auction aggregator named Bidders' Edge, to obtain an injunction forbidding Bidders' Edge from electronically "crawling" the eBay site with automated computer querying programs, or robots, to obtain auction information, without eBay's permission.[146] eBay argued that it had put Bidders' Edge on notice that its access was unauthorized, both via express (traditional) communication and via eBay's attempts to block the Bidders' Edge program electronically.[147] Accepting eBay's claim that it had suffered a trespass to chattels, the district court entered the requested injunction despite observing that the harm alleged, if any existed, was speculative and depended solely on the potential for harm if the injunction were denied.[148] Mere unwanted "use" of the plaintiff's computer, in the form of unwanted ac-

---

mass mailings of unsolicited commercial electronic mail, or "spam." Trespass ideas were initially invoked to prevent these unwanted signals from "encroaching," as it were, on the computer systems of Internet service providers ("ISPs") and on the mailboxes of harassed users. *See* Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1277 (N.D. Iowa 2000); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 452 (E.D. Va. 1998); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1020–27 (S.D. Ohio 1997).

[144] *See, e.g.*, eBay, Inc. v. Bidders' Edge, Inc., 100 F. Supp. 2d 1058, 1068–72 (N.D. Cal. 2000); Intel Corp. v. Hamidi, 114 Cal. Rptr. 2d 244, 247–52 (Ct. App. 2001), *review granted*, 43 P.3d 587 (Cal. 2002); *Register.com*, 126 F. Supp. 2d at 238, 249–51.

[145] *See, e.g.*, *eBay*, 100 F. Supp. 2d at 1068–74; *Intel*, 114 Cal. Rptr. 2d at 247–52; *Register.com*, 126 F. Supp. 2d at 238, 249–51.

[146] 100 F. Supp. 2d at 1062–63.

[147] *Id.* at 1068. eBay posted an electronic notice on its source code of its Web pages in the format known as the "robot exclusion header," a sort of electronic notice detectable to robot programs (and to anyone else examining the source code of the pages), which requested, but did not mandate, that robots observe a "stay away" request. *Id.* at 1061. More formally, the Standard for Robots Exclusion is a technical standard that permits Web page programmers to provide a notice, in the source code of each page, stating that the page should or should not be open for indexing and searching by automated software programs, such as those used by search engines to compile their databases. Robots programmed to comply with the Standard will observe the notice and not search or index pages with header information; robots not so programmed will ignore the notice. Information about the Standard for Robots Exclusion is available at http://www.robotstxt.org (last visited Nov. 15, 2002).

[148] *eBay*, 100 F. Supp. 2d at 1070–72. The *eBay* court cited two similar cases, but neither of those courts had based a finding of liability solely on the possibility of future harm. *See CompuServe*, 962 F. Supp. at 1015, 1022; Thrifty-Tel v. Bezenek, 54 Cal. Rptr. 2d 468, 475 (Ct. App. 1996).

cess to the information available at eBay's Web site, was sufficient, in other words, to justify the injunction.[149]

Register.com, Inc. v. Verio, Inc. involved a claim for trespass to chattels, among other theories, by Register.com, an Internet domain name registrar, against an Internet service provider that electronically "crawled" the plaintiff's online WHOIS database of domain name registration information, using what the court referred to as a "search robot."[150] Verio was using e-mail, telephone, and address information about domain name registrants to solicit prospective customers of Verio's Web hosting business, as prohibited by a notice posted on the Register.com Web site and in competition with Register.com.[151] The district court granted the requested injunction, citing the *eBay* decision, on the ground that the defendant had, by posting the Terms of Use provision on its Web site and by bringing the lawsuit itself, sufficiently indicated its intention that the defendant (and others using equivalent technology) were not welcome to "crawl" the plaintiff's system.[152] Noting that the plaintiff's argument for damages was weak to nonexistent, the court nonetheless found harm sufficient to justify a trespass-to-chattels claim, based on the risk of *future* interruption to the defendant's computer system.[153]

Most recently, an intermediate appellate court in California affirmed a grant of a permanent injunction on a trespass-to-chattels theory.[154] In *Intel Corp. v. Hamidi,* Intel sought to enjoin the defendant, a disgruntled former employee of the company, from sending unsolicited e-mail to current Intel employees.[155] The trial court issued the injunction and the appellate court affirmed, on the ground that Hamidi's e-mail messages traversed Intel's computer system without

---

[149] *See eBay*, 100 F. Supp. 2d at 1070–71; *see also* Oyster Software, Inc. v. Forms Processing, Inc., No. C-00-0724JCS, 2001 WL 1736382, at *11–13 (N.D. Cal. Dec. 6, 2001) (refusing to grant summary judgment against claim of trespass to chattels because plaintiff sufficiently presented evidence of unpermitted use of its computer system by defendant's robot program).

[150] 126 F. Supp. 2d at 241–43.

[151] *Id.* at 243–44.

[152] *See id.* at 249. The court described a notice posted to the plaintiff's Web site regarding appropriate terms of use as significant to its reasoning, but it noted that the defendant's robotic searching did not violate any of the terms of the notice. *See id.* No breach of contract claim was possible, and the defendant's lack of authority to search the database was primarily inferred from the fact of the plaintiff's lawsuit itself. *See id.*

[153] *Id.* at 250.

[154] *Intel*, 114 Cal. Rptr. 2d at 252.

[155] *Id.* at 246.

Intel's consent.[156] Intel was damaged by virtue of the accumulated distraction suffered by employees who opened and then discarded the messages.[157] According to the court, "Hamidi refused to respect Intel's request to stop invading its internal, proprietary e-mail system by sending unwanted e-mails to thousands of Intel's employees on the system."[158] As a result, "Intel proved more than its displeasure with Hamidi's message, it showed it was hurt by the loss of productivity caused by the thousands of employees distracted from their work and by the time its security department spent trying to halt the distractions."[159]

The Internet-as-place metaphor has not been solely responsible for these developments, but it unquestionably provides significant assistance to their doctrinal acceptance.[160] The argumentative value of the metaphor is simple. To modern courts and commentators, a violation of property boundaries is a trespass.[161] The owner of a parcel of real property has a nearly absolute power to exclude trespassers.[162] The owner of an electronic parcel of "real property" ought to have an equivalent power.[163] The courts are seizing on what they perceive to be the Internet's physical characteristics.[164] Characterizing the Internet as a place, or collection of places, reinforces the idea of bounda-

---

[156] *Id.* at 247, 249–50.

[157] *Id.* at 252.

[158] *Id.*

[159] *Intel*, 114 Cal. Rptr. 2d at 250.

[160] The most thoughtful analysis and critique of the trespass-to-chattel phenomenon, written before the cases discussed in the text were decided, proposes a nuisance-based formulation of access control (primarily in support of anti-spam regulation). *See* Dan L. Burk, *The Trouble With Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 53–56 (2000); *see also* Maureen A. O'Rourke, *Competition on the Internet: Who Owns Product and Pricing Information?*, 53 VAND. L. REV. 1965, 2001–05 (2000) (also advocating nuisance-based balancing test access control regime); Richard Warner, *Border Disputes: Trespass to Chattels on the Internet*, 47 VILL. L. REV. 117, 157–59 (2002) (recommending reasonable person standard for implied consent in trespass cases).

[161] As opposed to its more nuanced common-law sense of "invasion of a protected property interest."

[162] *See, e.g.*, *eBay*, 100 F. Supp. 2d at 1066 (citing Kaiser Aetna v. United States, 444 U.S. 164, 176 (1979)).

[163] *See id.*

[164] *Id.* at 1067 (stating that if eBay's computer system "were a brick and mortar auction house with limited seating capacity, eBay would be entitled to" reserve seats for bidders, refuse entrance to non-bidders, and seek relief against trespassers).

ries in a colloquial sense, and boundaries can be (but should not be) transgressed.[165]

It is obvious from this description that courts, at best, have misused the Internet-as-place metaphor by confusing access to "places" that represent information with access to the physical computer hardware that underlies computer systems. There is a metaphorical slipperiness here, a mixing of levels of abstraction, which courts seem happy to indulge. *eBay* provides the best example of the phenomenon.[166] The "chattel" at issue was the physical hardware operated by the plaintiff.[167] The "intermeddling" with the chattel was the unwanted sending of electronic signals "onto" or "into" the chattel by the defendant, an act that (even if repeated frequently) does no damage to the chattel, even if it does consume "bandwidth" (the ability of eBay servers to communicate with other networked computers—i.e., an intangible) and thereby does damage to eBay's bank account.[168] The defendant "wrongfully" accessed information that was valuable not at the signal (electron, or bit) level, but only at the human-readable level, prices being quoted for different items up for auction. In other words, the wrongful access took place at the Web *site* level, whereas the court indulged the plaintiff's theory of trespass to the *server*.[169] The Internet-as-place metaphor bridged the logical gap between the actual harm (the former) and the legal harm (the latter).

---

[165] The court in *eBay* specifically analogized eBay's claim to that of an owner of real property, in determining that preliminary injunctive relief was an appropriate remedy. *See id.*

[166] At least until the California Supreme Court issues its opinion in *Intel*. Intel Corp. v. Hamidi, 43 P.3d 587, 587 (Cal. 2002) (granting review of *Intel*, 114 Cal. Rptr. 2d 244).

[167] *eBay*, 100 F. Supp. 2d at 1063.

[168] *Id.* at 1062. "eBay's claim is that [Bidders' 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." *Id.* at 1071. The chattel, the server or collection of servers, is designed precisely to accommodate high volume, repeated surges of electronic signals. As one of the few profitable electronic commerce ventures on the Internet, eBay is perhaps uniquely aware of the need to maintain a large bank of robust computers. eBay's reaction to spiders on its servers evokes that of Captain Renault in the film *Casablanca*:

> **Renault:** Everybody's to leave here immediately. This café is closed until further notice. Clear the room at once.
> **Rick Blaine:** How can you close me up? On what grounds?
> **Renault:** I'm shocked, shocked to find that gambling is going on in here.
> **Croupier:** Your winnings, sir.
> **Renault:** Oh. Thank you very much. Everybody out at once.

CASABLANCA (Warner Brothers 1942).

[169] *See eBay*, 100 F. Supp. 2d at 1070.

The court's premise was a fair one. eBay claimed injury to its business based on alleged unfair competition by Bidders' Edge.[170] The injury consisted of damage to a slippery intangible, the information contained on eBay's Web site. To deal with that injury, the court focused on something easier to grasp, both literally and legally: eBay's computer equipment.[171] The court might legitimately have concluded that Bidders' Edge exceeded permitted access to the computer if and to the extent that the court intended to conclude, albeit indirectly, that Bidders' Edge was competing unfairly with eBay. That route was not the one that the court took; instead, the court focused on the transgression of the electronic boundary as wrongful in itself.[172] What began as a technique of protecting computers from information delivered from the outside has become not only a technique for protecting the information that the computers already contained, but a tool for protecting that information regardless of the actual harm sustained. What started as solicitude for injury suffered by proprietors of computer networks has become a tool for enforcing the perceived absolute right of the property owner to exclude unwanted visitors. As in real property trespass cases, the "injury" derives not from actual harm to the premises but from the proprietor's loss of the right to set the terms and conditions of entry.[173] Harm to informational interests themselves is not relevant.

Reliance on the Internet-as-place metaphor facilitated this transition, by essentially abandoning two significant requirements of com-

---

[170] *Id.* at 1063.

[171] *Id.* at 1071.

[172] *Id.* at 1070–71.

[173] *See id.* at 1073 (holding that Bidders' Edge's representatives are enjoined from crawling eBay's Web site without written authorization). In the real property context, there may be a good reason for connecting injury to an intangible interest (the right to exclude) to injury to a tangible interest (theft of a tangible thing), if the letter of the law does not support liability for the latter but injury to the former is clear. *See* People v. Kwok, 75 Cal. Rptr. 2d 40, 48–49 (Ct. App. 1998) (holding that defendant who made copy of key to victim's house was properly convicted of theft of property, within section 484 of the California Penal Code, because victim was not permanently deprived of tangible property, but was permanently deprived of exclusive control over access to her home). Retail stores occasionally try to enforce nominal policies stating the right to exclude individuals who are merely collecting comparative price information. *See, e.g.*, Culhane v. State, 668 S.W.2d 24 (Ark. 1984) (applying criminal trespass statute to employee of discount competitor of complainant Wal-Mart, who refused to leave store after being asked to do so); Mosher v. Cook United, Inc., 405 N.E.2d 720 (Ohio 1980) (rejecting civil action by consumer against store that had him arrested for trespassing). To the extent that these cases uphold anticompetitive behavior regarding price information, their reasoning seems questionable. *See* Desnick v. Am. Broad. Co., 44 F.3d 1345, 1351 (7th Cir. 1995).

mon-law trespass-to-chattels claims and thereby converting trespass to chattels into the kind of strict liability regime that effectively characterizes trespass to land. First, a trespass to chattel involves provable harm to the chattel.[174] In the world of physical property, the requirement has the sensible function of assuring that the plaintiff has a legal interest worth vindicating and can prove the extent of the harm, and also assuring that the defendant has a reasonable opportunity to avoid causing the injury.[175] In the world of interests in information, the property owner has two interests, one intangible and one tangible. Thoughtful application of trespass law in the present context would focus on the true nature of the plaintiff's injury, and on the counterpart interest of the defendant in avoiding that injury. Yet none of the courts discussed above give more than scant attention to requiring proof of actual harm to the chattel itself, or to notice to the defendant of the likelihood of that injury.[176] The Internet-as-place metaphor allows courts to conflate intangible and tangible injury, and allows the court to avoid a difficult inquiry into the character of the former.

Second, the doctrine clearly includes the requirement that the trespass be intentional.[177] The *Restatement* formulation of the rule requires proof of knowledge that "intermeddling" with the chattel will likely result, or that the defendant's activity is intended to intermeddle or interfere with the use of the chattel itself.[178] From the *Restatement* it appears that mere notice that the plaintiff does not consent to the intermeddling is not sufficient to demonstrate intent.[179] An alternative, less strict interpretation would treat the intent requirement as it is treated in cases of trespass to land, as a means merely of distin-

---

[174] *See eBay*, 100 F. Supp. 2d at 1071.

[175] *See id.* (quoting RESTATEMENT (SECOND) OF TORTS § 218 cmt. e (1965)).

[176] Courts' failure to analyze the question of harm in recent trespass-to-chattels cases has been well-described elsewhere. *See* Maureen A. O'Rourke, *What the Future Holds: Policy Choices in the Global E-Marketplace*, 7 ROGER WILLIAMS U.L. REV. 151, 160–61 (2001).

[177] *See, e.g.*, Zaslow v. Kroenert, 176 P.2d 1, 7 (Cal. 1946); RESTATEMENT (SECOND) OF TORTS § 217 (1965).

[178] *See* RESTATEMENT (SECOND) OF TORTS § 217 (1965); *see also supra* note 141 and accompanying text.

[179] As the California Supreme Court said regarding the related tort of conversion, "To establish a conversion, it is incumbent upon the plaintiff to show an intention or purpose to convert the goods and to exercise ownership over them, or to prevent the owner from taking possession of his property." *Zaslow*, 176 P.2d at 7; *see also* Itano v. Colonial Yacht Anchorage, 72 Cal. Rptr. 823, 827 (Ct. App. 1968), *cited with approval in eBay*, 100 F. Supp. 2d at 1070 (noting that trespass to personal property requires proof of both intent and lack of consent). The court in *Pritikin v. Liberation Publications, Inc.*, 83 F. Supp. 2d 920, 923 (N.D. Ill. 1999), discussed but did not decide whether the tort of conversion requires proof of a type of intent that proof of copyright infringement does not.

guishing claims for "intentional" or "knowing" harm from claims for negligence.[180] None of the three cases discussed above acknowledge intent as a separate element of the claim, other than to note that the plaintiff did not consent to the defendant's activity.[181] If the second interpretation of the intent requirement is the correct one, then the courts may have it right. "Intent" means absence of consent, either *ex ante* or *ex post*. Then again, perhaps not. Even if the defendant committed a knowing or volitional act, that act was directed not at the chattel, but at the information located "at" (or "on," or "in") the chattel. By ignoring this distinction here, too, the doctrine has taken on the cast of trespass to land, where even innocent invasions of the landowner's property interest justify relief. If the actual (if unacknowledged) harm to the plaintiff is damage to an interest in information, and the likely intent of the defendant is to inflict that harm (though presumably the defendant believes that it is engaging in lawful competition), the omission of a meaningful intent requirement with respect to the chattel itself effectively converts trespass to chattels on the Internet into a strict liability offense—as a claim of trespass to land is ordinarily understood to be.

C. *Anti-Circumvention and the DMCA*

The Internet-as-place metaphor appears in less explicit ways in the DMCA.[182] The anti-circumvention provisions of the DMCA were enacted in 1998 to enhance the remedies available to owners of copyrighted works in the electronic network environment. The DMCA provides civil remedies and the possibility of criminal penalties for two related acts.[183] First, the act of circumventing a "technological measure that effectively controls access" to a copyrighted work is prohibited under section 1201(a)(1)(A).[184] "[T]o 'circumvent a technological measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copy-

---

[180] Prosser and Keeton recognize that the authorities diverge. *See* W. PAGE KEETON, DAN B. DOBBS, ROBERT E. KEETON & DAVID G. OWEN, PROSSER AND KEETON ON THE LAW OF TORTS § 14, at 86–88 (5th ed. 1984).

[181] *See, e.g.*, *eBay*, 100 F. Supp. 2d at 1062.

[182] *See* Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as scattered sections of 17 U.S.C.).

[183] 17 U.S.C. §§ 1201–1203 (2000).

[184] *Id.* § 1201(a)(1)(A).

right owner."[185] "[A] technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."[186] A related provision of the statute forbids "trafficking" in anti-circumvention technology.[187] A second provision prohibits trafficking in technology that is primarily designed for the purpose of circumventing technological protection measures that effectively protect a right of a copyright holder.[188] "Any person" injured by a violation of sections 1201 or 1202[189] has standing to sue.[190] No threshold of harm need be established.[191] The act of circumventing, or trafficking in the circumvention technology, constitutes the violation.[192]

Colloquially speaking, these provisions were designed to help electronic information proprietors "lock up" their content, in the face of the dangers that the Internet (with its ease of high-speed anonymous remote access) heralded.[193] The DMCA, in other words, was supposed to help information proprietors keep out thieves and pirates by giving legal cover to their efforts to secure information technologically.[194] Copyright law alone would not be enough because electronic copying is easy to accomplish and difficult to detect.[195] Click-through agreements would be insufficient protection on the ground that the legal framework surrounding their enforceability was of uncertain strength, and sanctions for breach of contract provided insufficient deterrence to outright theft.

Like trespass to chattels in the electronic environment, the DMCA did not begin as a doctrine of access control. The legislative

---

[185] *Id.* § 1201(a)(3)(A).

[186] *Id.* § 1201(a)(3)(B).

[187] *Id.* § 1201(a)(2).

[188] *See* 17 U.S.C. § 1201(b)(1)(A). A parallel definition of circumventing "protection afforded by a technological measure" appears in 17 U.S.C. § 1201(b)(2)(B). It appears that the act of circumventing a technological protection measure that effectively protects a right of a copyright holder is not unlawful under the DMCA, if one can lawfully acquire a device that permits doing so.

[189] Section 1202 addresses maintaining the "integrity of copyright management information." *See id.* § 1202.

[190] *Id.* § 1203(a).

[191] *See id.* § 1201.

[192] *See id.* § 1201(a)(1)(A), (b)(1)(A).

[193] *See* S. REP. No. 105-190, at 2, 8 (1998).

[194] *See* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519, 555–56 (1999).

[195] *See* S. REP. No. 105-190, at 2, 8.

history of the statute is relatively clear in its reliance on place-based metaphors (a sibling of the Internet-as-place metaphor) in support of the major goal of excluding thieves and pirates.[196] According to the *House Report* that accompanied the final bill, "The act of circumventing a technological protection measure put in place by a copyright owner to control access to a copyrighted work is the electronic equivalent of breaking into a locked room in order to obtain a copy of a book."[197] The *Senate Report* likewise analogized the prohibition on trafficking in anti-circumvention technology to "making it illegal to break into a house using a tool, the primary purpose of which is to break into houses."[198] The better reading of the statute itself draws a distinction between claims made under section 1201(a)(1) and (2), which prohibit circumventing and trafficking in technology designed to circumvent access controls (controlling the user's initial access to the work), and section 1201(b)(1), which prohibits trafficking in technology that permits circumventing controls guarding the rights of the copyright holder, or copy controls (controlling what the user does with the work after initial access).[199] The metaphors used in connection with Congress's anti-piracy rhetoric most clearly support only the former.

In practice, the darker themes suggested by these place metaphors have been softened. The metaphors have been applied in service of doctrinal claims that information proprietors may use the DMCA to control access to information, whether or not real "piracy" is threatened. In *Universal City Studios, Inc. v. Corley*, the first major judicial decision interpreting (and upholding, against constitutional challenge) the anti-circumvention provisions of the DMCA, the U.S. Court of Appeals for the Second Circuit affirmed a permanent injunction entered by the district court forbidding a Web site owner from providing live links to online sources of a computer program known as DeCSS.[200] The program allowed consumers to watch DVD-formatted motion pictures on computers and other machines not configured with the CSS encryption standard used by motion picture studios.[201] The DeCSS program permitted "circumvention" of a

---

[196] *See* H.R. REP. No. 105-551, pt. I, at 17 (1998); S. REP. No. 105-190, at 11.

[197] H.R. REP. No. 105-551, pt. I, at 17.

[198] S. REP. No. 105-190, at 11.

[199] 17 U.S.C. § 1201(a), (b) (2000).

[200] 273 F.3d 429, 434–35 (2d Cir. 2001).

[201] *Id.* at 435–36. The essence of the plaintiffs' claims is captured in the court's statement, "DeCSS is designed to circumvent 'CSS,' the encryption technology that motion

"technological measure" protecting copyrighted works, within the meaning of the DMCA, specifically because it permitted consumers to view copyrighted motion pictures without the express authorization of the copyright owners (as expressed in the CSS technology).[202] Within the statutory framework, the case was decided and affirmed primarily under section 1201(a)(2), forbidding trafficking in technology defeating access controls.[203] (The plaintiff also alleged a claim under section 1201(b)(1), prohibiting trafficking in circumvention technology aimed at copy controls.)[204] That is, the DeCSS program was a forbidden access control technology even if it were used by a lawful owner of a DVD to watch that DVD on computer devices not equipped with CSS.[205] Repeated viewing of the movie by a consumer on an unapproved device would constitute unauthorized access. This departure from the reading of the statute suggested above was rationalized via metaphor.[206] Reasoning from the place metaphor originally developed to punish the true pirate, the Second Circuit wrote:

> Owners of all property rights are entitled to prohibit access to their property by unauthorized persons. Homeowners can install locks on the doors of their houses. Custodians of valuables can place them in safes. Stores can attach to products security devices that will activate alarms if the products are taken away without purchase. These and similar security devices can be circumvented. Burglars can use skeleton keys to open door locks. Thieves can obtain the combinations to safes. Product security devices can be neutralized.
>
> Our case concerns a security device, CSS computer code, that prevents access by unauthorized persons to DVD movies. The CSS code is embedded in the DVD movie. Access to the movie cannot be obtained unless a person has a device, a licensed DVD player, equipped with computer code capable of decrypting the CSS encryption code. In its basic function,

---

picture studios place on DVDs to prevent the unauthorized viewing and copying of motion pictures." *Id.* at 435–36. The extent to which the defendant was accused of facilitating unauthorized distribution of motion pictures via DeCSS was debated, *see id.* at 438 n.5, and was ultimately not material to the court's conclusion that the DMCA forbids distribution of the DeCSS technology. *See id.* at 444.

[202] *See id.*

[203] *See id.* at 441–43.

[204] *See id.* at 441.

[205] *See Corley*, 273 F.3d at 441.

[206] *See id.* at 452–53.

> CSS is like a lock on a homeowner's door, a combination of a safe, or a security device attached to a store's products.
>
> DeCSS is computer code that can decrypt CSS. In its basic function, it is like a skeleton key that can open a locked door, a combination that can open a safe, or a device that can neutralize the security device attached to a store's products. DeCSS enables anyone to gain access to a DVD movie without using a DVD player.[207]

The case did not involve access to information available solely or even primarily on the Internet. The congruity between the court's use of an "information-as-thing" metaphor (the forbidden DeCSS code enables users to "break into" information in a container) and an Internet-as-place metaphor is, however, unmistakable.[208] To the court, information "protected" by access control technology is located in a house, or in a store, places, to be sure, even if not necessarily "located" on the Internet.[209] This reasoning can be seamlessly extended to electronic networked information; metaphorically, a computer network or a Web site is no more or less a "place" than a DVD that consists of a "home" or a "store."[210] The court made clear that the DMCA empowers the information proprietor[211] to regulate access to information based on an absolute place-based understanding of the electronic information environment. Moreover, the court made clear that its concern in applying the DMCA was with the injury to the place itself, rather than to the underlying information: "[T]he DMCA targets the circumvention of digital walls guarding copyrighted material (and trafficking in circumvention tools), but does not concern

---

[207] *Id.*

[208] *See id.*

[209] *See id.*

[210] In one sense, invoking "home" as a metaphorical analog here ups the ante, since both colloquially and in real property law "homeowners" have nearly absolute rights to control access. Disney's home, as it were, is its castle. *Cf.* Lexmark Int'l, Inc. v. Static Control Components, Inc., No. 02-CV-571, 2003 WL 912614, at *24 (E.D. Ky. Feb. 27, 2003) (holding that DMCA creates both right to protect object and right to protect work.)

[211] The scope of the DMCA is formally limited to copyrighted works. 17 U.S.C. § 1201(a)(1)(A) (2000) (stating that anti-circumvention protection applies to works protected under Title 17 of the United States Code), (b)(1)(A) (stating that protection extends to circumvention that effectively protects a right of a copyright owner). It was argued in *Corley* that in practice, and as interpreted in the district court, the DMCA enables "locking up" of public domain works. *See Corley*, 273 F.3d at 445. The Second Circuit refused to consider the argument on the ground that the argument was not properly presented. *See id.*

itself with the use of those materials after circumvention has occurred."[212]

In other cases interpreting the DMCA, it is clear that the metaphor-inspired conversion of the DMCA from a piracy-prevention measure to a commercial access control measure is not limited to offline settings. In *RealNetworks, Inc. v. Streambox, Inc.*, the manufacturer of computer technology used to format "streams" of audio for transmission over the Internet, sued a distributor of technology that enabled a consumer to "capture" those streams in permanent form and to convert the streamed format into alternative formats.[213] "Streaming" music files using RealNetworks technology permits the distributor of that music to specify, technologically, that a consumer who listens to the stream over the Internet cannot download or otherwise save a copy of the entire computer file containing the work.[214] That technological specification includes two components: a "Secret Handshake" that permits the audio stream to be transmitted only to a computer program distributed by RealNetworks known as the RealPlayer, and the "Copy Switch," which specifies whether or not the streamed

---

[212] *See Corley*, 273 F.3d at 443; *see also* Sony Computer Entm't of Am. v. Gamemasters, 87 F. Supp. 2d 976, 987 (N.D. Cal. 1999) (enjoining sale of GameEnhancer device that permitted consumers to bypass geographical limitations built into Sony PlayStation console games and to play such imported games without Sony's permission; decided under § 1201(a)(2)); Michael Landau, *Has the Digital Millennium Copyright Act Really Created a New Exclusive Right of Access?: Attempting to Reach a Balance Between Users' and Content Providers' Rights*, 49 J. COPYRIGHT SOC'Y U.S.A. 277, 289–90 (2001). In *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1122–25 (N.D. Cal. 2002), the district court refused to dismiss criminal DMCA charges against a firm that distributed a computer program that permitted consumers to de-crypt the text of "electronic books" made available via proprietary "reader" software that otherwise prevented consumers from making electronic copies of the underlying text, modifying that text, or printing copies of that text. The prosecution was brought under section 1202(b) of the DMCA, which prohibits "trafficking" in technology that permits circumvention of technological measures that effectively protect "a right of a copyright owner" under Title 17. *See* 17 U.S.C. § 1201(b). This section of the DMCA does not validate access controls in the same way as section 1201(a). Instead, it appears to prohibit technology that defeats technical limits on reproducing, distributing, or preparing derivative versions of works to which consumers already have legitimate access, i.e., copy control technologies. *See Elcom*, 203 F. Supp. 2d at 1120–21. But as interpreted, an enforceable technological control on use becomes, in effect, an enforceable condition of access. *See id.* at 1124–25 (concluding that Congress intended to ban all anti-circumvention technologies, regardless of their purpose); Dan L. Burk, *Anti-Circumvention Misuse*, UCLA L. REV. (forthcoming 2003), *draft available at* http://ssrn.com/abstract_id=320961; Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1643–44 (2002).

[213] No. 2:99CV02070, 2000 WL 127311, at *1 (W.D. Wash. Jan. 18, 2000).

[214] *Id.* at *2.

audio file may be saved and/or copied.[215] The defendant's technology permitted the consumer to bypass both and to retain a digital copy of the work, using a program other than the RealPlayer.[216] Ruling on the plaintiff's request for a preliminary injunction under sections 1201(a) (with respect to the Secret Handshake) and 1202(b) (with respect to the Copy Switch) of the DMCA, the court granted the request.[217]

It is true that only in the *Corley* decision was a court, in applying the DMCA, expressly influenced by the statute's place-based metaphorical framework.[218] The influence of the framework appears elsewhere in a subtle but significant respect that closely resembles flaws in application of trespass-to-chattels doctrine. Trespass-to-chattels cases have proceeded with little concern that prospective defendants might not be able to discern the difference between legitimate and illegitimate entry, that is, between injury to a tangible interest and injury to an intangible one. Courts in DMCA cases have seized on the "locked house" metaphor without measuring it against the actual effectiveness of the "locks" found in the real world or asking whether legally protecting the "lock" gets at the interest that the plaintiff is trying to protect.[219] Here the influence of the information-as-thing metaphor is much in evidence; the Internet–as-place (or electronic-environment-as-place) metaphor is implicit. Under the DMCA, weaker locks, and houses that do not appear to be locked, get at least as much legal pro-

---

[215] *Id.*

[216] *Id.* at *4.

[217] *See id.* at *7–9. The case clearly involved application of the DMCA as access control rather than "piracy prevention." As the court characterized the plaintiff's claim:

> Copyright owners also use RealNetworks' technology so that end-users can listen to, but not record, music that is on sale, either at a Web site or in retail stores. Other copyright owners enable users to listen to content on a "pay-per-play" basis that requires a payment for each time the end-user wants to hear the content. Without the security measures afforded by RealNetworks, these methods of distribution could not succeed. End-users could make and redistribute digital copies of any content available on the Internet, undermining the market for the copyrighted original.

Id. at *3.

[218] To the extent that the Internet-as-place and information-as-thing represent efforts to physicalize purely intangible phenomena, the vocabulary of *RealNetworks* (the Secret Handshake, the defendant's Streambox VCR device, the Copy Switch) is highly sympathetic. The court compared the defendant's technology to a "black box" that could be used to intercept and descramble cable or satellite television signals. *RealNetworks*, 2000 WL 127311, at *4.

[219] Arguably, this is a manifestation of the absence of the Internet-as-place metaphor, since one might expect to see greater emphasis on genuine gates or fences by courts enamored of the physical analogy. The paradox, then, is that courts rely on the metaphor.

tection as do good, strong locks. And the lock itself appears to be a protected interest, even though the underlying information is what the plaintiff is truly trying to guard. In both respects, prospective defendants have legitimate concerns regarding notice of their potential liability.

Both the U.S. District Court for the Southern District of New York, in its opinion in *Corley*, and the U.S. District Court for the Western District of Washington, in its opinion in *RealNetworks*, ruled that a "technological measure" may "effectively" protect against the unauthorized access to or copying of copyrighted works (and therefore qualify the plaintiff for DMCA relief) even if the technological access barrier imposed can be evaded with relative ease.[220] In *RealNetworks*, the court reasoned that the plaintiff's technology was intended to prevent capture and copying of the digital audio files themselves, even if the copyrighted works could be easily captured and copied by other (non-digital) means.[221] The effectiveness of the technological measure related, in other words, to a tangible attribute of the plaintiff's product (its electronic format), or information-as-thing, rather than to the intangible copyright interest that the DMCA nominally protects.[222] The district court in *Corley* more directly relied on the place metaphor in its analysis of this issue, by analogizing distributing the DeCSS program to publishing the combination to a bank vault.[223]

D. *The Computer Fraud and Abuse Act*

Like click-through agreements, for the information proprietor the DMCA has its weaknesses as an access control technique. The information proprietor must invest in at least a trivial "technological protection measure" before the provisions of the DMCA can be invoked.[224] More important, the DMCA encompasses only wrongful ac-

---

[220] *See* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317–18 (S.D.N.Y. 2000), *aff'd sub nom.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001); *RealNetworks*, 2000 WL 127311, at *9; *cf.* Samuelson & Scotchmer, *supra* note 212, at 1646–48 & n. 333 (describing how DMCA stunts competitive incentives to produce truly effective technological protection measures).

[221] *See RealNetworks*, 2000 WL 127311, at *9.

[222] The defendant could, therefore, plausibly argue that the intangible copyrighted work was subject to no access or rights control whatsoever.

[223] *See Reimerdes*, 111 F. Supp. 2d at 315.

[224] The DMCA plaintiff also must contend with limited statutory exceptions for reverse engineering, security testing, and encryption research, *see* 17 U.S.C. § 1201(f), (g), (j) (2000), and with arguments that the statute is unconstitutional. *See Corley*, 273 F.3d at 458 (rejecting First Amendment challenge).

cess to copyrighted works and invasion of the rights of copyright owners. Information not protected by copyright law formally falls outside the statute. To fill these gaps, information proprietors have begun recently to enforce access restrictions by relying on the federal CFAA.[225] The CFAA generally provides both criminal penalties and civil relief in connection with claims of unauthorized access to a "protected computer."[226] Originally enacted before the commercial development of the Internet in order to help secure government and related special-purpose computers from hackers, the CFAA now reaches many different kinds of unauthorized access to almost any computer connected to the Internet.[227] As with the law of trespass to chattels, the CFAA was originally designed to keep "bad" information (and people) out,[228] rather than "good" information in, by denying competitors and consumers access except on the proprietor's terms. As with the trespass cases, the law has expanded to cover both situations. The Internet-as-place metaphor has helped the cause of those who rely on the CFAA to control unauthorized "access" not only to computer systems themselves, but to the information that those computers contain.

For ordinary civil liability purposes, the CFAA applies to anyone who: (1) "intentionally accesses a computer without authorization or exceeds authorized access [and thereby obtains] information from any protected computer if the conduct involved an interstate or foreign communication;"[229] (2) "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a pro-

---

[225] *See* 18 U.S.C. § 1030 (2000), *amended by* USA Patriot Act of 2001, Pub. L. 107-56, § 814, 115 Stat. 272, 382–84, 21st Century Department of Justice Appropriations Authorization Act, Pub. L. No. 107-273, § 4002, 116 Stat. 1758, 1807–08 (2002), and Homeland Security Act of 2002, Pub. L. No. 107-296, § 225, 116 Stat. 2135, 2158.

[226] A "protected computer" under the statute includes a computer "which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." *Id.* § 1030(e)(2)(B).

[227] Brief histories of the CFAA are provided in Eric J. Bakewell et al., *Computer Crimes*, 38 AM. CRIM. L. REV. 481, 487–95 (2001), and Dodd S. Griffith, Note, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 455–66 (1990).

[228] *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 524–26 (S.D.N.Y. 2001) (dismissing CFAA claim that defendant placed "cookies" on computers of Internet site visitors); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125–26 (W.D. Wash. 2000) (stating that disloyal employee's theft of trade secrets from employer's computer system supported CFAA liability); *LCGM*, 46 F. Supp. 2d at 451–52 (treating sending of spam as CFAA violation).

[229] 18 U.S.C. § 1030(a)(2).

tected computer;"[230] (3) "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage;"[231] (4) "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;"[232] or (5) "by conduct described in . . . subparagraph (A) [(2)–(4) above], caused (or, in the case of an attempted offense, would, if completed, have caused)—(i) loss to 1 or more persons during any 1-year period aggregating at least $5,000 in value."[233]

The civil relief provision of the CFAA provides: "Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."[234] An Internet-connected computer resource is a "protected computer."[235] Reduced to its essence, therefore, the CFAA authorizes a civil claim (and raises the possibility of criminal prosecution) against anyone who accesses a computer connected to the Internet without the permission of its owner and causes at least $5,000 worth of "loss."[236]

Despite its anti-hacking origins,[237] the CFAA, and subsections 1030(a)(2) and 1030(a)(5) in particular, appears on its face to justify interpreting the statute as an access-control regime in the same commercial law sense as the law of trespass to chattels and the DMCA. As with those two areas, that interpretation does not distinguish between wrongful access to the computer system itself, on the one hand, and to the information stored on it, on the other. Access is wrongful if it is

---

[230] *Id.* § 1030(a)(5)(A).

[231] *Id.*

[232] *Id.*

[233] *Id.* § 1030(a)(5)(B)(i). The civil liability subsections of the CFAA were modified slightly by the USA Patriot Act of 2001 to clarify that the $5,000 threshold can be satisfied only by damage caused by a single act. *See* Pub. L. 107-56, § 814, 115 Stat. 272, 382–84.

[234] 18 U.S.C. § 1030(g). The balance of this subsection reinforces the substantive prerequisites for a civil claim: "A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B)." Subsection (i) is quoted in the text above. Subsections (ii) through (v) address physical injury and damage to public health, safety, and security.

[235] *Id.* § 1030(e).

[236] *See id.* § 1030.

[237] *See* United States v. Czubinski, 106 F.3d 1069, 1078 (1st Cir. 1997) (holding that intention of CFAA felony provisions is to punish attempts to steal valuable data, not to punish mere unauthorized access); N. Tex. Preventative Imaging, L.L.C. v. Eisenberg, No. SA CV 96-71AHS(EEX), 1996 WL 1359212, at *4–*6 (C.D. Cal. Aug. 19, 1996) (finding that 1994 CFAA amendments shifted statutory focus to the defendant's intent, from unauthorized access itself, under section 1030(a)(5)).

"without authorization" or "exceeds authorized access."[238] Whose authority counts for CFAA purposes? Authority of the owner of property rights in the target computer, or in a computer system involved in the access? Or authority of the owner of property rights in the information acquired? Either, or both? It appears that courts have not paid close attention to these distinctions.[239] As with trespass to chattels doctrine and the DMCA, the Internet-as-place metaphor has reinforced this muddiness and enhanced the CFAA's standing as a budding commercial law regime. For example, in *Register.com* the plaintiff included a claim under subsections of the CFAA that prohibited unauthorized access to a protected computer that caused damage[240] and that led to obtaining information.[241] The U.S. District Court for the Southern District of New York entered a preliminary injunction, based in part on its finding that the plaintiff was likely to succeed on its CFAA claim of obtaining information without authorization.[242] Recently, in *EF Cultural Travel BV v. Explorica, Inc.*, the U.S. Court of Appeals for the First Circuit held that accessing a competitor's Web site using a robot or spider program to collect price information from the site, in order to use that information to offer competitive services (overseas tours for student groups), made out a CFAA violation.[243] The court affirmed entry of a preliminary injunction by the district court.[244]

---

[238] 18 U.S.C. § 1030(a)(2).

[239] *See, e.g.*, United States v. Morris, 928 F.2d 504, 509–10 (2d Cir. 1991) (stating that computer use is "without authorization" if it is not in any way related to the intended function of the computer); Doe v. Dartmouth-Hitchcock Med. Ctr., No. CIV 00-100-M, 2001 WL 873063, at *5–6 (D.N.H. July 19, 2001) (physician accessing patient records potentially liable under CFAA for exceeding scope of authority granted by physician's employer); *LCGM*, 46 F. Supp. 2d at 451 (CFAA violation made out when spam e-maile-mail sent to AOL accounts in violation of plaintiff's customer agreement with AOL and AOL Terms of Service). At least one court has distinguished use of the concept of "access" under the CFAA from its cousin in trespass, implying, among other things, that "implied consent" or "implied license" is no defense to a CFAA claim. *See In re* Am. Online, Inc., 168 F. Supp. 2d 1359, 1370 n.8 (S.D. Fla. 2001).

[240] 18 U.S.C. § 1030(a)(5)(A)(iii); *Register.com*, 126 F. Supp. 2d at 241.

[241] 18 U.S.C § 1030(a)(2)(C); *Register.com*, 126 F. Supp. 2d at 241. This subsection refers to the unauthorized obtaining of information from a protected computer. The USA Patriot Act made clear that civil claims for violation of this subsection can be brought only if the plaintiff also establishes a violation of 18 U.S.C. § 1030(a)(5)(B).

[242] *See Register.com*, 126 F. Supp. 2d at 251–53.

[243] 274 F.3d 577, 579, 582–85 (1st Cir. 2001). The injunction entered by the district court was based on, and affirmed with respect to, 18 U.S.C. § 1030(a)(4), which prohibits unauthorized access to a protected computer, and thereby obtaining anything of value, "with intent to defraud." *Id.* at 582 n.10, 583–84.

[244] *Id.* at 583–84.

The court's reliance on Internet-as-place reasoning in *Explorica* is, given the prior review of trespass and DMCA cases, unsurprising. The computer program used by the defendants was known as a "scraper," because its object was to "scrape" up information on the target Web site. The court also described the misbehavior of the program as it "mined" the plaintiff's Web site and "navigated" the Web site structure.[245] What is moderately surprising is how clearly the opinion relies on the metaphor while giving no weight to how that metaphor fails to capture the challenged practice.[246] Proving a CFAA violation requires, among other things, that the defendant have accessed the "protected computer" without authorization or by exceeding authorization.[247] The basis for the First Circuit's finding that the defendant did not have authority to access the plaintiff's site was a confidentiality agreement executed by one of the defendants, as a former employee of the plaintiff.[248] Because the data that the defendants used to program the "scraper" were allegedly "confidential" within the meaning of the confidentiality agreement, which covered EF Cultural Travel's secret technical, business, or financial information, their access to the plaintiff's computer was "unauthorized."[249] But was it? The technical data concerned access to (or in truth, use of) the information stored on the Web site, rather than access to the computer itself. Nothing that the defendants did exceeded their authorized access to the computer. The computer was freely accessible by anyone with the ability to use the Internet. Had the plaintiff brought a lawsuit for misappropriation of trade secrets, the claim might well have been rejected. The technical information was publicly displayed to anyone who browsed price data on the plaintiff's Web site.[250] A trade secrets claim at least would have addressed the merits of what the defendants allegedly did wrong. By re-characterizing the defendant's acquisition of competitive information as "unauthorized access" under the CFAA ("breaking in" to a protected area, "navigating" around it, and "mining" it for its valuables) rather than "misappropriation of trade secrets" (allegedly unethical competitive conduct), the court conflated access to the

---

[245] *See id.* at 583.

[246] *See id.* at 583–84.

[247] *See supra* notes 229–233 and accompanying text.

[248] *See Explorica*, 274 F.3d at 582.

[249] *See id.*

[250] To avoid this point, the court concluded that the "confidential" data obtained by the defendant by virtue of his employment enabled the scraper to collect information much more quickly than another individual could. *See id.* at 583 n.16.

physical with access to the virtual. The plaintiff was able to obtain an injunction against a lower-cost competitor, at essentially no cost to itself.[251]

A companion case, decided a little over a year later, avoids some of the most pronounced metaphorical errors discussed above without, in the end, solving the underlying problem. In that regard, the case provides a useful transition to the discussion in the next Part. In *EF Cultural Travel BV v. Zefer Corp.*, the Court of Appeals for the First Circuit addressed the same underlying facts presented in *Explorica*.[252] The defendant, Zefer, produced the software used in the "unauthorized" scraping and had been named as a defendant in the initial litigation.[253] Though not named as a party subject to the initial preliminary injunction, affirmed in *Explorica*, Zefer appealed the injunction as applied to its activities.[254] The appeal was delayed by its intervening bankruptcy proceeding.[255] When the bankruptcy stay was lifted, the appeal proceeded.[256] Reviewing the injunction a second time, the First Circuit affirmed it again, on the narrow ground that Zefer, like any third party with notice of the injunction, was prohibited from acting in concert with or at the direction of Explorica to use the scraper tool to access EF Cultural Travel's price information.[257] The court thus had no need to address again the metaphorical concerns that buttressed its earlier ruling.

Nonetheless, in dicta, the court offered significant guidance for future application of the CFAA. As noted in *Explorica*, the district court entered the preliminary injunction by reasoning that the defendants had exceeded the "reasonable expectations" of both the Web site owner and its users.[258] As applied to Explorica, the court affirmed the injunction without addressing this "reasonable expectations" interpretation.[259] As applied to Zefer, the court seized the opportunity to declare that the standard was justified neither by the language of

---

[251] The plaintiff provided little or no advance notice that it had withdrawn permission to browse its site, and it offered no technical resistance to the operation of the "scraper" itself. *See id.* The court declined to rule on the adequacy of any "no access" notice posted by the plaintiff. *See id.*

[252] 318 F.3d 58, 59–60 (1st Cir. 2003).

[253] *Id.* at 60–61.

[254] *Id.*

[255] *Id.* at 61.

[256] *Id.*

[257] *See Zefer*, 318 F.3d at 63–64.

[258] *Explorica*, 274 F.3d at 580–81.

[259] *Id.* at 583–84.

the statute nor by good public policy.[260] Instead, the court suggested that the Web site owner could withdraw authority to visit the site by using an explicit notice—or link—on the relevant Web page or Web site, stating what uses are forbidden:

> [W]e think that the public website provider can easily spell out explicitly what is forbidden and, consonantly, that nothing justifies putting users at the mercy of a highly imprecise, litigation-spawning standard like 'reasonable expectations.' If EF wants to ban scrapers, let it say so on the webpage or a link clearly marked as containing restrictions.[261]

This dicta does not depend, even to the extent that the earlier opinion in *Explorica* did, on explicit characterizations of the plaintiff's Web site and the defendants' activities as involving improper access to a physical place or tangible thing. (An implicit acceptance of this usage continued. The court noted that the case involved a "scraper tool,"[262] and that the plaintiff's Web site was designed to require that users view "only one page at a time.")[263] Yet the court continued its conflation of concerns over injury to intangible interests in information and injury to tangible interests in computer systems. The court went out of its way to acknowledge the public nature of the plaintiff's Web site as a whole and of all of the price information that it contained.[264] The court went further, noting that copyright and unfair competition laws would likely prevent the plaintiff even from using an explicit notice to prevent Zefer from simply viewing that information as would an "ordinary" user.[265] If a future defendant in Zefer's position were to ignore such a "no scraping" notice by viewing publicly available information on the plaintiff's Web site using a "scraper tool," what would be the nature of the injury? It could only be an injury framed in terms of injury to a tangible interest—the Web site, or the Internet, as place—wrought by a tangible thing, the "scraper tool." The continuing (implicit) recognition of the Internet-as-place metaphor in this context might be contrasted with the different use of that

---

[260] *Zefer*, 318 F.3d at 63.

[261] *Id.* Elsewhere in the opinion, the court noted that public policy might limit the nature of such restrictions. *See id.* at 62.

[262] *See id.* at 60.

[263] *Id.* at 62.

[264] *See id.* at 60.

[265] *See Zefer*, 318 F.3d at 63.

metaphor by the Second Circuit in *Specht*.[266] Bypassing a "no scraping" notice merely posted on a Web site might be enough, under *Zefer*, to sustain civil liability under the CFAA.[267] With respect to a contract claim, under *Specht*, bypassing an equivalent notice would not support liability.[268]

III. Access and the Shape of the Internet

The foregoing critique of recent cases decided under the CFAA, the DMCA, and the doctrine of trespass to chattels, argues that courts have erred by relying on an Internet-as-place metaphor without properly connecting that metaphor to interests in intangible information that have been at issue. By contrast, cases applying contract and commercial law to click-through agreements have, over time, recognized (at least formally) both producer and consumer interests in intangibles, without adopting a persuasive metaphor. A bit of doctrinal and metaphorical consistency is in order, to the extent that these doctrines address the same commercial interests and to the extent that the metaphor carries substantial descriptive weight.[269] This Part assumes that the overlap of commercial interests, implicit in the previous Part, will cause the reach of these doctrines to continue to expand. It also assumes that the Internet-as-place metaphor will continue to be far more descriptively powerful than any alternative for transactions in information. It argues, then, that a more effective understanding of this metaphor can help these different doctrines work more consistently.

Others have argued that courts have erred because their use of an Internet-as-place metaphor has not been sufficiently sensitive to nuances in legal doctrines governing use of and access to land.[270] The error may run more deeply. Courts have not appreciated *why* the land metaphor lacks the absolutist dimension that they often assume, or, to put the matter differently, how the metaphor maps onto individuals' perceptions of the world and thus supports a much more elaborate argumentative vocabulary than courts have recognized. In the real

---

[266] *See supra* notes 110–127 and accompanying text.

[267] *See Zefer*, 318 F.3d at 63–64.

[268] *See supra* notes 110–127 and accompanying text.

[269] *See generally* Harvey S. Perlman, *Interference with Contract and Other Economic Expectancies: A Clash of Tort and Contract Doctrine*, 49 U. Chi. L. Rev. 61 (1982) (arguing that tort and contract doctrines should be interpreted consistently when applied to the same acts, when policy objectives coincide).

[270] *See* Hunter, *supra* note 27; Lemley, *supra* note 42.

world, property is understood and used in context-specific ways. Over time, the limits supplied by context are embodied in law,[271] and enrich our vocabulary of property. By failing to tap into that context- and experience-based vocabulary, courts using the simplest form of the Internet-as-place metaphor are imposing legal rules that do not resonate in our experience of the Internet and that are not, therefore, likely to have whatever effect on our behavior that courts intend. Instead, if the Internet is a place of metaphorical real property, property-like regulation should be based on how its users understand and use it.

How do we understand and appreciate the "place" that is the Internet? If the Internet were really a place, what would it look like? Or how would those people who "live," "work," or "play" there describe it? Physical environments have objective, describable physical characteristics. Real property law reflects user experience with them. It is a relatively straightforward (if somewhat technical) matter to map the physical characteristics of the Internet.[272] In the offline world, a seminal study concluded forty years ago that the physical reality of the place may not be as important to its inhabitants as their understanding of that reality.[273] What makes a place a "place" is a combination of features, some mappable using objective techniques, many others constituted by individuals through their experience of "using" the place.[274] Implicitly, the law of a place will reflect these perceptions at least as much as, if not more than, those features themselves.

In this study, Kevin Lynch and a team of researchers from the Massachusetts Institute of Technology undertook to interview inhabitants of three cities (Boston, Massachusetts; Jersey City, New Jersey; and Los Angeles, California) to learn about their "readings," or maps, of those cities.[275] The goal of the research was to determine how people constituted the physical environment they occupied.[276] What did they identify as landmarks in their lives, the boundaries of their territory or neighborhood?[277] What did they understand as "public" and

---

[271] *Cf.* Carol Rose, *The Comedy of the Commons: Custom, Commerce, and Inherently Public Property*, 53 U. CHI. L. REV. 711, 779–81 (1986).

[272] *See supra* note 46 (pointing out distinctions among "layers" of the Internet).

[273] Surprisingly, perhaps, given the nature of the findings, the study has not been repeated.

[274] *See* KEVIN LYNCH, THE IMAGE OF THE CITY 2, 8–13 (1960); JOSEPH RYKWERT, THE SEDUCTION OF PLACE: THE CITY IN THE TWENTY-FIRST CENTURY 133 (2000).

[275] LYNCH, *supra* note 274, at 14.

[276] *Id.* at 2.

[277] *See id.* at 140–41, 43–85.

"private" spaces and categories inbetween?[278] The results, published as *The Image of the City,* revealed, as the scholar Joseph Rykwert later argued, that "[p]oints of orientation are essential for any sane urban or rural living. Without them a citizen cannot 'read,' let alone 'understand' his home."[279] Lynch's research identified certain common and important themes: "[I]f the environment is visibly organized and sharply identified, then the citizen can inform it with his own meanings and connections. Then it will become a true *place,* remarkable and unmistakable."[280] The organization and distinction typically derived from an inventory of features and boundaries includes open space, contrasts, and a sense of motion.[281] Paths, edges, nodes, landmarks, and distinct districts played key roles to Lynch's subjects.[282] Taken together, the degree to which these features were present in a given physical environment was a measure of its "imageability," a term that Lynch defined as "that quality in a physical object which gives it a high probability of evoking a strong image in any given observer. It is that shape, color, or arrangement which facilitates the making of vividly identified, powerfully structured, highly useful mental images of the environment."[283] An "imageable" city was a city that conveyed a coherent mental map to its inhabitants, that its inhabitants could understand and use to organize their lives, and that enabled them to realize their potential as citizens.[284] From the urban planning standpoint, the benefits of a more highly imageable environment were the potential it yielded for productive development and exploration by individual citizens.[285]

Lynch's research was designed to encourage urban planners to develop imageable places.[286] Its implications go further. A cognitive

---

[278] *See id.*

[279] RYKWERT, *supra* note 274, at 133. Rykwert goes on to contrast the variety of experience represented in Lynch's study with the "standardization of space" represented by late twentieth-century capitalism.

[280] LYNCH, *supra* note 274, at 92.

[281] *Id.* at 16.

[282] *Id.* at 46–49.

[283] *Id.* at 9. "A highly imageable (apparent, legible, or visible) city in this peculiar sense would seem well formed, distinct, remarkable; it would invite the eye and the ear to greater attention and participation." *Id.* at 10.

[284] *See id.* at 108–10.

[285] *Cf.* LYNCH, *supra* note 274, at 108–10, 119.

[286] Information researchers have for some time been exploring how to adapt the imageability idea to the Internet. *See, e.g.,* Matthew Chalmers et al., *Adding Imageability Features to Information Displays, in* PROCEEDINGS OF THE 9TH ANNUAL ACM SYMPOSIUM ON USER INTERFACE SOFTWARE AND TECHNOLOGY 33, 33–38 (Ass'n for Computing Mach., Inc.,

approach to metaphor argues that our use of language depends in large part not on objective reality but on our understanding of that reality.[287] Metaphor is not merely language. It reflects a system of thought.[288] It follows that whatever the influence of language on law, that influence should follow our understanding of the sources of that usage. Any other relationship creates a needless risk of our legal structures failing sufficiently to correspond to other social structures, a sort of cognitive dissonance on a grand scale. As Part II showed, the Internet-as-place metaphor has a deeper impact on law than in merely suggesting ways to talk about the Internet. Our uses of the language of place reflect our understanding of place.[289] As courts' use of the place metaphor has informed the law, a correct understanding of the metaphor can help repair some of the resulting errors. The Internet may not be, nor should it be, a wholly imageable place in Lynch's sense.[290] As imageability is a useful way to think about our physical places, the idea of imageability provides a useful starting point for discussing how to adapt the benefits of a place metaphor to the Internet. "Imageability," or designing a user environment so that users can comprehend it, is important not only to the idea of personal growth and exploration (the argument from urban planning), but to the idea of a coherent environment for economic and commercial development.[291]

If the Internet, or the relevant commercial and/or technical context, lacks imageability, to borrow Lynch's term, or significant "boundaries," in a more accessible sense, it is hardly fair *or efficient* to impose what is in law or in practice a regime of strict liability for wrongful access to a *computer* when the harm alleged is misuse or ap-

---

UIST '96 Symposium, 1996), *available at* http://doi.acm.org/10.1145/237091.237096; Younghee Jung & Alison Lee, *Design of Social Interaction Environment for Electronic Marketplaces, in* CONFERENCE PROCEEDINGS ON DESIGNING INTERACTIVE SYSTEMS: PROCESSES, PRACTICES, METHODS AND TECHNIQUES 129, 129–36 (Ass'n for Computing Mach., Inc., DIS '00 Symposium, 2000), *available at* http://doi.acm.org/10.1145/347642.347690. For an overview of the field of Human-Computer Interaction (HCI), see the resources collected at ACM/SIGCHI, at http://www.acm.org/sigchi (last visited Mar. 14, 2003).

[287] *See supra* notes 25–36 and accompanying text.

[288] *See supra* notes 25–36 and accompanying text.

[289] *See supra* notes 25–36 and accompanying text.

[290] *See* LYNCH, *supra* note 274, at 9.

[291] *See* Wendy J. Gordon, *An Inquiry into the Merits of Copyright: The Challenges of Consistency, Consent, and Encouragement Theory*, 41 STAN. L. REV. 1343, 1380 (1989) ("In short, an interdependent world requires demarcations to avoid paralysis and preserve valuable, mutually beneficial reciprocities.").

propriation of valuable *information*.[292] To the extent that courts and Congress are concerned about wrongful or anticompetitive use of information, and want to influence user behavior to limit misuse, then the way in which the Internet-as-place metaphor has been used to date misses that goal entirely. If the relevant interest in access cases is truly the information stored "on" the Web site, then the problem created by current usage of the Internet-as-place metaphor is that prospective defendants typically have little effective way to "see" the liability that they may later confront, because they cannot "see" the Internet or its boundaries. Defendants are punished for invading plaintiff's place-like "property" without necessarily being aware that they have committed a wrong.[293] Develop significant boundaries in some sense, and the Internet becomes visible. It acquires a shape, from the user's perspective. The Internet-as-place metaphor becomes more than just metaphor. It resonates in practice. The place metaphor acquires meaning.

Giving substance to the Internet-as-place metaphor from the user's perspective is appropriate at the least because those who access information on the Internet, and are bound by the regulatory schemes described above, are entitled as a matter of simple fairness to have the language that courts and legislatures invoke to define their experience match that experience itself. Both the choice of user perspective and place as the source of metaphorical meaning make sense

---

[292] Previous arguments of this sort have advocated that the law do more to balance owner and user interests. *See* O'Rourke, *supra* note 41; *cf.* Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. (forthcoming 2003), *draft available at* http://ssrn.com/abstract_id=310020 (arguing that legal questions concerning the Internet may be analyzed differently depending on the choice of a "reality-based" (external) or "virtual-reality-based" (internal) perspective).

[293] *See, e.g.*, *supra* notes 150–153, 243–251 and accompanying text. Johnson & Post wrote:

> Treating Cyberspace as a separate "space" to which distinct law apply [sic] should come naturally. There is a "placeness" to Cyberspace because the message access [sic] there are persistent and accessible to many people. Furthermore, because entry into this world of stored online communications occurs through a screen and (usually) a password boundary, you know when you are "there." No one accidentally strays across the border into Cyberspace.

Johnson & Post, *supra* note 3, at 1379 (footnotes omitted). Their last point may be true, although it precedes my argument. No one accidentally strays into cyberspace, but once "in" cyberspace, it is all too easy to stray across hidden boundaries. *Cf.* WILLIAM J. MITCHELL, CITY OF BITS: SPACE, PLACE & THE INFOBAHN 151 (1995) ("The great power struggles of cyberspace will be over network topology, connectivity, and access—not the geographic borders and chunks of territory that have been fought over in the past.").

from other policy perspectives.[294] One might argue that the primary concern of information policy is preservation and content of the public domain.[295] In that event, information resources ought not to be privatized without good reason; inadequate boundary-making blurs the public/private distinction and puts the public domain at unnecessary risk. Such an instrumental argument might be reversed (and courts invoking Internet-as-place and contract-as-assent metaphors have, when relying on policy justifications, tended to do so),[296] but with the same result. Inadequate boundary-making means that information producers will have imperfect and potentially inadequate incentives to produce information. One might view property and assent as ends in themselves,[297] a perspective that supposes defined and definable property rights, and conditions that permit the exercise of autonomous choice by the individual. Boundary-making enables both.

In the doctrinal context, boundary-making means making people aware of the boundaries that exist, whether those boundaries are physical, logical, or legal.[298] A technical boundary—a rights management scheme, for example—would not automatically be sufficient if it did not effectively communicate the existence of a boundary to the user. Imageability and visibility are cultural phenomena, not inevitable or natural consequences of certain tangible features. In the nonelectronic world, tangible boundaries perform this function, in the information environment as well as elsewhere, but their effectiveness derives not just from their tangible nature but also from our cultural understanding of what physical barriers mean.[299] Common sense sug-

---

[294] *See* Orin S. Kerr, *Are We Overprotecting Code? Thoughts on First-Generation Internet Law*, 57 WASH. & LEE L. REV. 1287, 1289–90 (2000) (arguing for greater focus on function of Internet technology, rather than on the essential technical form of the technology, in analysis of Internet legal problems); Timothy Wu, *Application-Centered Internet Analysis*, 85 VA. L. REV. 1163, 1163–66 (1999) (arguing for regulatory framework based on character of application programs used on the Internet, because the character of different applications affects user perceptions of the character of cyberspace).

[295] *See* Benkler, *supra* note 9, at 354 (arguing that baseline in law regulating information, including creative works, should be that they are "free as the air to common use," citing Justice Brandeis's famous dissenting opinion in *International News Service v. Associated Press*, 248 U.S. 215, 250 (1918) (Brandeis, J., dissenting)).

[296] *See, e.g.*, *supra* notes 86–106, 146–149 and accompanying text.

[297] *See* Barnett, *supra* note 37, at 291–319.

[298] *Cf.* Benkler, *supra* note 46.

[299] *See* Gordon, *supra* note 291, at 1354–94 (arguing that the legal boundaries provided by the rules of the 1976 Copyright Act largely serve the same functions as the physical boundaries of tangible property, under pre-1976 law); *see also supra* note 46 and authorities discussed therein.

gests that one ought not to be held liable for an offense in the absence of some rational basis for imputing knowledge that harm may result or that an offense may be committed, and for identifying the harm that results from the violation.[300] In the context of each of the four bodies of law reviewed in Part II, and for any equivalent body of law brought to bear on the question of unauthorized "access" to information and computer resources, courts should require that the plaintiff or party that wishes to enforce any type of access limitation bear the burden of establishing the existence of a relevant feature of the information environment that creates, with respect to some significant number of users of that environment, a salient or visible boundary between open, public information and information subject to access constraints. Giving actual notice of the access restriction to the individual user may not be sufficient. Such a notice may be presented in a form or context that lacks salience or visibility from the user's perspective, and thus fails to correspond in any meaningful way to what courts describe as the user's experience of the Internet-as-place. From a policy perspective, enforcement of a particular term or feature might arguably be fair, or efficient, or properly instrumental in its effect with respect to a particular user, but there is no reason to assume that like conditions apply with respect to all users. The plaintiff, in other words, should establish not merely notice, but imageability, from the user's perspective. To employ legal rather than planning terminology, the plaintiff should prove foreseeability *from the perspective of the user.* If a significant number of users cannot foresee the potential harm from exceeding an alleged access control, or see the Internet, the individual user ought not to be held accountable for breaches of legal standards governing access to Internet resources. The next Part of this Article explores and explains this proposal.

---

[300] Ignorance of the law may be no excuse, as the proverb says, but liability is rarely imposed absent some rational basis for concluding that the defendant (or the accused) should have been aware that legal consequences attached to its conduct. *See* Intercon, Inc. v. Bell Atl. Internet Solutions, Inc., 205 F.3d 1244, 1247–48 (10th Cir. 2000) (holding that defendant "purposefully availed" itself of state's law when it continued to route e-mail traffic through servers located in that state after notice of harm caused by such routing). *But see* Verizon Online Servs., Inc. v. Ralsky, 203 F. Supp. 2d 601, 619–20 (E.D. Va. 2002) (finding personal jurisdiction in Virginia over defendants accused of trespass to chattels caused by spam, despite absence of evidence in the record that defendants knew that plaintiff's servers were located there); State v. Maxwell, 767 N.E. 2d 242, 247, 250 (Ohio 2002) (The court reinstated the conviction for importing child pornography over the dissent of J. Lundberg Stratton, who wrote: "[C]harging individuals with the knowledge of the internal workings of their Internet service provider is repugnant to fairness and due process.").

IV. A Law of Access

The term "foreseeability" is meant to capture in legal terms the idea that if a plaintiff wants to erect barriers to access to information, and to rely on physical space metaphors to enforce those barriers legally, then that plaintiff ought to be required to signal to potential defendants that their conduct is potentially wrongful.[301] In cases of trespass to land, it is said that the wrongful entry by the defendant must be "intentional," in the sense that the defendant must be shown to have intended to be where the defendant was found.[302] Landowners have no obligation to post signs or build fences as a condition of recovering for trespass, but the clarity of their entitlement to eject trespassers must stem from the likelihood that the trespasser either actually knows, or is in an excellent position *ex ante* to determine, whether entry is authorized.[303] In cases of virtual access, a foreseeability standard substitutes for that clarity.[304] Although not intended to import all of the complexity and subtlety of foreseeability analysis from tort law, the standard does evoke the tort-law foreseeability in-

---

[301] In other areas of law involving intellectual property and involving the Internet, a foreseeability standard has been suggested recently as a preferred way of managing competing producer and consumer interests. *See* Matthew J. Conigliaro et al., *Foreseeability in Patent Law*, 16 Berkeley Tech. L.J. 1045, 1064–68 (2001) (summarizing uses of foreseeability doctrine in patent law as well as in tort and contract law); Michael A. Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 Berkeley Tech. L.J. 1345, 1380–84 (2001) (arguing in favor of a "targeting criterion" for questions of personal jurisdiction involving Internet-related contacts); *see also* Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co., Ltd., 535 U.S. 722, 740–41 (2002) (largely adopting foreseeability standard for equivalents analysis in patent law).

[302] *See* Nat'l Coal Bd. v. I.E. Evans & Co., 2 K.B. 861, 865 (C.A. 1951), *available at* 1951 WL 11384 (English court reviewing evolution away from regime of strict liability and holding that defendant was not liable in trespass for harm to an underground cable which he nonnegligently struck while excavating in a field); Keeton et al., *supra* note 180, § 13, at 73–74. Negligent invasion of land will support a claim of trespass, but as a practical matter such a claim will sound directly in negligence.

[303] *See* Ian Ayres, *Protecting Property With Puts*, 32 Val. U. L. Rev. 793, 829 (1998) ("When Rose steals my watch or builds an encroaching wall or becomes a holdover tenant, Rose usually knows at the time that she is unlawfully impairing my entitlement. In contrast, it is more difficult for Rose to know in advance whether her noise or dust emission will constitute a nuisance."). Economic models similarly distinguish between trespass and nuisance generally on the ground that the former arises in contexts where transactions costs between the parties are low. *See* William M. Landes & Richard A. Posner, The Economic Structure of Tort Law 42–48 (1987); Thomas W. Merrill, *Trespass, Nuisance and the Costs of Determining Property Rights*, 14 J. Legal Stud. 13, 23–26 (1985).

[304] Cases of trespass to land that do not involve classic interference with possession have at times, and for similar reasons, relied on a similar balancing approach to gauge the reasonableness of the defendant's conduct. *See* Martin v. Reynolds Metals Co., 342 P.2d 790, 794–96 (Or. 1959).

quiry. More specifically, it evokes the notion that in the absence of a considered determination that a regime of strict liability is appropriate,[305] a defendant ordinarily ought to be liable to a plaintiff only for conduct that the defendant can either plan to avoid, or for which the defendant (and the court) can calculate (and perhaps obtain insurance for) compensation.[306] The goal in this Part, then, is to use the foreseeability standard to harmonize application of the four areas of law described in Part II. Our thinking, language, and law about virtual places should mirror their equivalents in the world of real places. A foreseeability standard implements that argument in a unified way, across doctrinal lines.

There are two important points to emphasize in this context. First, because much of the rest of this Part discusses clear or effective barriers and boundaries, I do not mean to argue that a technologically robust boundary is either necessary or sufficient, in every case, to warrant imposing liability for exceeding that boundary. The question, instead, is whether the boundary is implemented in a way that fairly signals to information users that they are crossing a legally significant boundary. Second, I use the term "foreseeability" to unify the doctrinal suggestions that follow, but I do not propose that a literal foreseeability requirement be added in any particular doctrinal sense. Doctrinally, foreseeability is foreign to the question of the existence of an enforceable agreement, and to interpretation of the DMCA and the CFAA. As trespass is a tort, foreseeability is a related concept, but in tort law foreseeability is related to the defendant's intent, and traditional trespass-to-chattels (and trespass-to-land) doctrine recognizes the concept of "intent" in only a limited way.[307] The link among the four doctrines, and between the doctrines and foreseeability, lies at the level of interests, rather than doctrine, and particularly in the interest in regulation of access to information.[308] All four doctrines ad-

---

[305] *See generally* Alfred C. Yen, *A Personal Injury Law Perspective on Copyright in an Internet Age*, 52 HASTINGS L.J. 929 (2001) (considering policies supporting strict liability in personal injury in the context of claims for copyright infringement).

[306] In some of the cases discussed above, it appears likely that the plaintiffs were willing to accept some level of access by the defendants but could not, without litigation, persuade the defendants to pay the desired price. *See, e.g.*, eBay v. Bidders' Edge, Inc., 100 F. Supp. 2d 1058, 1062 (N.D. Cal. 2000).

[307] *See* RESTATEMENT (SECOND) OF TORTS § 217 cmt. c (1965); KEETON ET AL., *supra* note 180, § 13, at 73–74; *see also supra* notes 141, 177–180, 301–303 and accompanying text.

[308] To the extent that each doctrine addresses a distinct interest, then boundaries between the doctrines ought to be preserved, even reinforced, rather than eliminated. *See* O'Rourke, *supra* note 41, at 686. Common usage of place-and-space metaphors, and sub-

dress that interest mostly as a tort interest.[309] The plaintiffs in each of the cases described above argue that the defendants breached a duty not to access the plaintiffs' information without permission.[310] The source of the duty may have been contractual, statutory, or explicitly based in tort.[311] In none of these areas does the evidence or the doctrine suggest that a regime of true strict liability (liability without fault and without actual or constructive knowledge of ensuing harm) is appropriate.[312] Yet uncritical reliance on the Internet-as-place metaphor has pushed courts strongly in that direction. By encouraging reliance on "visible" restrictions on access, the foreseeability standard preserves application of the metaphors, in the context of an appropriate and consistent application of the law. The rest of this Part describes how the foreseeability concept could be accommodated in existing doctrines, and responds to some anticipated criticisms.

A. *Applications*

1. Click-Through Agreements

Click-through doctrine, at least as described through the *Specht v. Netscape Communications Corp.* decision, now recognizes the importance of a foreseeability concept, even if it does not do so in so many words.[313] Moreover, the manner in which the court in *Specht* concluded that the information provider (Netscape) could not enforce an agreement to arbitrate closely tracks the sense in which I argue

---

stantially overlapping application of access-regulating sources of law, suggest that with respect to access and use of information itself, harmonization is the better course.

[309] *Cf.* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 452–53 (2d Cir. 2001) (describing breach as circumvention of locked door in DMCA suit); ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1450 (7th Cir. 1996) (describing breach in context of contract claim not to access information); *eBay*, 100 F. Supp. 2d at 1068 (describing breach in context of trespass to chattels by accessing information).

[310] *See, e.g.*, *Corley*, 273 F.3d at 452–53; *ProCD*, 86 F.3d at 1450; *eBay*, 100 F. Supp. 2d at 1068.

[311] *See, e.g.*, *Corley*, 273 F.3d at 452–53; *ProCD*, 86 F.3d at 1450; *eBay*, 100 F. Supp. 2d at 1068.

[312] A strict liability regime is not a part of click-through contract law. *See* discussion *supra* Part II.A. Strict liability is not suggested in the DMCA, *see supra* notes 182–198 and accompanying text, or in the CFAA, *see supra* notes 224–236 and accompanying text. Neither is it suggested in the doctrine of trespass to chattels or trespass to land. *See supra* notes 141, 177–180, 301–303 and accompanying text.

[313] 306 F.3d 17, 29–31 (2d Cir. 2002); *see also supra* notes 125–127 and accompanying text.

that foreseeability implements a sense of visibility of the Internet.[314] The information users in *Specht* were not bound to Netscape's proposed agreement because that agreement was presented online without any contextual cues that signaled that proceeding further online constituted a legally significant act.[315] The fact that these users could download Netscape's software without being required to assent to a click-through mechanism was a compelling indicator that they were not presented with an opportunity to assent to Netscape's terms that was meaningful in the context of the transaction.[316] The technological mechanism that Netscape used (or failed to use) was not determinative.[317] More important was the fact that the users in this case did not have a vocabulary to understand the potential legal significance of their actions. *Specht,* in short, rightly focuses on the context of the information user's knowledge of and access to terms that the information proprietor might later rely on to limit that user's rights.[318]

A foreseeability analysis, in one sense, simply adopts the approach followed in *Specht.*[319] It also emphasizes a different dimension of the result in *Specht,* without relying so heavily on its doctrinal framework. The court in *Specht* was talking about assent, and using the absence of relevant context to draw a conclusion about whether the

---

[314] *See Specht,* 306 F.3d at 29–31; *see also supra* notes 125–127 and accompanying text.

[315] *See Specht,* 306 F.3d at 29–31; *see also supra* notes 125–127 and accompanying text.

[316] *See Specht,* 306 F.3d at 29–31; *see also supra* notes 125–127 and accompanying text.

[317] *See Specht,* 306 F.3d at 29–31; *see also supra* notes 125–127 and accompanying text.

[318] Effective arguments regarding the proper scope of federal preemption of copyright claims have been frustrated by courts' failure to require that non-preempted contracts regarding copyrighted works constitute genuine agreements. *ProCD v. Zeidenberg,* 86 F.3d 1447 (7th Cir. 1996), has been heavily criticized in the copyright community for its simplistic analysis of the argument that the contract claim in that case was preempted by federal copyright law. *See* Nimmer et al., *supra* note 68, at 42–60. *See generally* Maureen A. O'Rourke, *Copyright Preemption After the ProCD Case: A Market-Based Approach,* 12 BERKELEY TECH. L.J. 53 (1997). Scholars have urged that courts develop more sophisticated tools for understanding both preemption and related doctrines to limit claims of exclusive control over copyrighted works. *See generally* Mark A. Lemley, *Beyond Preemption: The Law and Policy of Intellectual Property Licensing,* 87 CAL. L. REV. 111 (1999).

[319] A variety of contracts scholars have argued that enforceability of terms in form contracts presented to consumers should be limited to "salient" or "visible" terms. *See* Barnett, *supra* note 48, at 637–39 (arguing for "radically unexpected terms" review of form terms, with respect to individual party); Russell Korobkin, *Bounded Rationality and Unconscionability: A Behavioral Approach to Policing Form Contracts,* 70 U. CHI. L. REV. (forthcoming 2003), *draft available at* http://ssrn.com/abstract_id=367172 (recommending enforcement of form terms that are visible to a significant number of buyers); Todd D. Rakoff, *Contracts of Adhesion: An Essay in Reconstruction,* 96 HARV. L. REV. 1174, 1251–53 (1983) (recommending enforcement of "visible" terms).

plaintiffs had assented to the terms proposed by Netscape.[320] Given the precedential material before the court, this is understandable, but it should be recognized that doctrinally the court is perpetuating the contract-as-assent metaphor. The case can be better understood as the right kind of application of the Internet-as-place metaphor. In this framework, Netscape would argue that the information users—including all those who visited the Netscape site, not just the plaintiffs—"went" someplace in order to access the Netscape software, and by going there implicitly recognized the limitations of that place.[321] According to the court, Netscape never signaled to those users that any significant change in venue had occurred.[322] For future contract-based disputes, therefore, a foreseeability standard derived from the Internet-as-place metaphor should be a useful tool supporting the type of substantive (if not metaphorical) analysis pursued in *Specht*.[323]

---

[320] *See Specht*, 306 F.3d at 29–31.

[321] In the context of certain common carrier agreements, a comparable rule, enforcing form terms only if they are presented to the consumer in a manner that reasonably communicated to the consumer notice of those terms, has been in place for many years. *See* Deiro v. Am. Airlines, Inc., 816 F.2d 1360, 1364 (9th Cir. 1987); Shankles v. Costa Armatori, S.P.A., 722 F.2d 861, 864 (1st Cir. 1983); Silvestri v. Italia Societa Per Azione Di Navigazione, 388 F.2d 11, 17 (2d Cir. 1968). The doctrine arose initially in the context of limitations on liability found in passenger tickets (and thus as a form of federal common law applied in maritime cases), and has been extended recently to limitations on liability offered by shippers. *See* Mudd-Lyman Sales & Serv. Corp. v. United Parcel Serv., 236 F. Supp. 2d 907, 910–11 (N.D. Ill. 2002); Shorts v. United Parcel Serv., No. CIVA3:97-CV-0682R, 1999 WL 118791, at *5 (N.D. Tex. Feb. 25, 1999), *aff'd*, 204 F.3d 1114 (5th Cir. 1999); Vieira v. United Parcel Serv., Inc., No. C-95-04697, 1996 WL 478686, at *1 (N.D. Cal. Aug. 5, 1996). Proof of "reasonable notice" requires meeting two standards. First, the proponent of the terms must show that notice was adequate given the physical characteristic of the ticket, including size of the type, conspicuousness of the terms, and clarity of the notice on the face of the ticket. *See Deiro*, 816 F.2d at 1364. Second, notice must adequate in light of the circumstances surrounding the passenger's purchase and retention of the ticket, including the customer's sophistication, time and incentives to consider the terms of the ticket, and any other notice that the customer received outside of the ticket itself. *Id.* The customer, under all the circumstances, must have had the ability to become meaningfully informed. *See id.*; Carpenter v. Kloster Rederi A/S, 604 F.2d 11, 12–13 (5th Cir. 1979); *Silvestri*, 388 F.2d at 17 ("[T]he thread that runs implicitly through the cases sustaining incorporation is that the steamship line had done all it reasonably could to warn the passenger that the terms and conditions were important matters of contract affecting his legal rights."). This line of cases has been all but ignored in analysis of shrinkwrap and click-through agreements. *But see generally* Kaustuv M. Das, Note, *Forum-Selection Clauses in Consumer Clickwrap and Browsewrap Agreements and the "Reasonably Communicated" Test*, 77 WASH. L. REV. 481 (2002).

[322] *See Specht*, 306 F.3d at 31.

[323] To take the example most likely to provoke debate in the near future, enforceability of browse-wrap "agreements," assent to browse-wrap terms may be inferred either by "use" of an information resource with "awareness" of terms of use, or by "acceptance" of the

2. Trespass to Chattels

The *Restatement (Second) of Torts*, on which the recent electronic trespass cases rely, requires that the defendant *intentionally* dispossess, use, or intermeddle with the plaintiff's chattel before liability may be imposed.[324] Courts have given lip service to the intentionality requirement in these cases, interpreting the requirement as courts traditionally have interpreted "intent" in the context of claims of trespass to land.[325] In *eBay, Inc. v. Bidders' Edge, Inc.*, the necessary intent was inferred from the fact that the defendant's automated search agent bypassed a "robots.txt" file (a non-mandatory electronic request embedded in the plaintiff's software that the defendant's software was at liberty, as a technological matter, to ignore),[326] and from the fact of the filing of the claim.[327] In *Intel Corp. v. Hamidi*, Hamidi's intent to trespass was demonstrated by Intel's giving him actual notice that he should not send e-mails "through" Intel's computer network.[328] Applying the foreseeability standard, the intent requirement should be made substantive. Intent would have to be shown by evidence that in the ordinary course of operating and using the plaintiff's computer

---

"benefit" of the resource along with implied limitations on that benefit. Each argument may be contested on traditional contract terms, because it can be fairly debated in each case whether an individual user manifested "assent" by "using" or taking the "benefit" of access to the information. The foreseeability standard would require an additional analytic step in this case, asking whether the information proprietor took steps to make users aware of any specific "use" or "benefit" of access to information limited by terms and conditions of access. It is typically far from clear that "visiting" a Web site, for example, that is, merely reading and surfing, consists of the sort of "use" of an information resource that would not be provided without implied terms and conditions. It cannot be presumed that information users understand that they receive an identifiable "benefit" from access to an electronic information resource that may appear to be free (as with much of the World Wide Web), or for which they may already have paid (as with access to the Internet via commercial service providers, or with copies of computer programs).

[324] RESTATEMENT (SECOND) OF TORTS § 217 (1965).

[325] In trespass-to-land cases, the plaintiff must show no more than that the defendant intended to be where the defendant was. *See supra* notes 301–303 and accompanying text.

[326] *See supra* note 147 and accompanying text (discussing operation of Standard for Robots Exclusion).

[327] 100 F. Supp. 2d at 1068–72.

[328] 114 Cal. Rptr. 2d 244, 250 (Ct. App. 2001), *review granted*, 43 P.3d 587 (Cal. 2002). An "actual notice" standard suggests that "constructive notice" might also suffice. In the electronic context, this may be even less fair to potential defendants, and even less consistent with the Internet-as-place metaphor. *See Specht*, 306 F.3d at 31 (declining to hold user to "constructive notice" of Netscape's offered terms). *But see* McLaren v. Microsoft Corp., 1999 WL 339015, at *4 (Tex. Ct. App. May 28, 1999) (finding that an employer "owned" an employee's personal e-mail messages in part because they were stored on a corporate computer network).

facilities, a significant number of users in the defendant's position necessarily knew or should have known that they were crossing some culturally significant boundary. Proof of service of a complaint (or delivery of a cease-and-desist demand) objecting to access by the defendant, standing alone, would be insufficient. Either of these forms of notice is no better than the evidence on which courts relied in *eBay* and *Intel*, for example. An electronic device or other technology designed to prevent such access, that did prevent such access, and that signaled in some way that access was prohibited, would suffice, but electronic devices, computer programs, and access keys and the like would not if they could be ignored or bypassed in the ordinary course of the user's attempting to obtain access to the information.

The difference between this proposal for the electronic environment and its equivalent in the physical environment (in which a "No Trespassing" sign or a cease-and-desist demand letter typically gives prospective trespassers adequate notice, if any is required, of an impending tort) is precisely the interest captured by the foreseeability standard. In real space, individuals encounter and are accustomed to encountering a variety of signs and signifiers that mark significant boundaries. A fence or a "No Trespassing" sign exists as part of a larger cultural vocabulary indicating, among other things, places that individuals may or may not, can and cannot, and should and should not, go. Absent a more pronounced rule for trespass on the Internet, no equivalent vocabulary is likely to arise.[329] A mere "No Trespassing" "sign" on the Internet, such as the robots.txt file relied on by the court in *eBay*, is easily ignored as a triviality on the Internet as a whole.

Claims for trespass to land do not formally require that the defendant have advance knowledge or notice of the plaintiff's property interest,[330] and in that respect the proposal goes beyond a mere analogy to existing trespass doctrine. To the extent that this doctrine in the land context is driven by an implicit argument about the relatively low cost to the defendant of obtaining information about the scope of the plaintiff's interest,[331] then extension of the foreseeability standard in the virtual realm is justified. It cannot safely be said that an infor-

---

[329] The rule thus both substitutes for missing imageability on the Internet and creates an incentive to develop one. The Standard for Robots Exclusion, for example, now permits only an "access/no access" signal that does not discriminate among different types of automated programs. Standard for Robots Exclusion, *at* http://www.robotstxt.org (last visited Nov. 15, 2002).

[330] *See supra* notes 140–141 and accompanying text.

[331] *See supra* note 303 and accompanying text.

mation user has at hand a low-cost, easily understood method of determining the scope of an information proprietor's rights.[332] The higher the user's information, the more the liability regime should require proof of the user's knowledge.

3. Anti-Circumvention and the DMCA

Section 1201 of the DMCA appears to be a "strict liability" regime for circumventing technical protection measures and for trafficking in anti-circumvention technology.[333] The accused defendant is liable if the evidence establishes that "effective" technical protection measures were circumvented, or anti-circumvention technology "designed or produced" for circumvention purposes or with "limited commercially significant" non-circumvention purposes was trafficked in.[334] There seems to be little room in the statutory text for a requirement that a potential defendant have advance knowledge of potential DMCA liability.[335]

The statute does require that the subject technical protection measure be "effective" before a remedy (for circumvention, or for trafficking) can be granted.[336] The meaning of "effective" is not perfectly clear. "Effective" has two, closely related statutory definitions.[337] First, in the context of access control technology, it means that "the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."[338] Second, in the context of copy control technology, it means that "the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title."[339] As noted above, courts have been extremely generous in their reading of these definitions.[340] The legislative history of the DMCA suggests that Congress was primarily concerned with large-scale piracy of copy-

---

[332] *See* Jessica Litman, *The Exclusive Right to Read*, 13 CARDOZO ARTS & ENT. L.J. 29, 34–35 (1994).

[333] *See* 17 U.S.C. § 1201 (2000); *see also supra* notes 182–198 and accompanying text.

[334] 17 U.S.C. § 1201(a)(2)(A), (B). The anti-trafficking statute is also violated if the defendant knows that the technology will be used to circumventtechnological protection measures.

[335] *See id.*

[336] *See id.* § 1201(a)(1)(A), (a)(2), (b)(1).

[337] *See id.* § 1201(a)(3)(B), (b)(2)(B).

[338] *Id.* § 1201(a)(3)(B).

[339] 17 U.S.C. § 1201(b)(2)(B).

[340] *See supra* notes 220–223 and accompanying text.

righted works.[341] Given the property metaphors on which Congress relied, it is reasonable, and consistent with what the legislative history reveals regarding Congressional intent, to argue that a property owner is entitled to strong protection against burglary to the extent that the owner has taken significant steps to safeguard the property within. Metaphorically, the door need not have three separate deadbolts and a steel frame, but there should be a door of some sort, the key should not be under the front mat, and the property should be behind it. A DMCA plaintiff cannot simply declare that something is a locked "house." That thing must signify "house" to the user community. A measure ought not to be "effective," and a remedy under the DMCA ought not to be available, if the plaintiff's technological measure can be defeated with relative ease. Giving real meaning to the effectiveness requirement would be an appropriate way to locate the foreseeability standard in the DMCA, because an "effective" technical protection measure would be, among other things, a measure that gives notice that significantly more than ordinary operation of the technology embodying or carrying the information is required to access the relevant information.[342]

4. The Computer Fraud and Abuse Act

Civil liability under the CFAA requires that the defendant have accessed the plaintiff's computer or computer network "knowingly" or "intentionally," "without authorization," or have exceeded "authorized access," and either caused the requisite harm or obtained information.[343] These terms beg the question of the type of evidence needed to demonstrate that the defendant "knew" that authority to access the plaintiff's computer system was lacking or "intended" to proceed despite a lack of access. Aside from dicta in *EF Cultural Travel BV v. Zefer, Corp.*,[344] courts in recent civil CFAA cases discussed above have

---

[341] *See* H.R. REP. No. 105-551, pt. I, at 17 (1998); S. REP. No. 105-90, at 11 (1998).

[342] A similar argument was rejected by the district court in *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 317–19 (S.D.N.Y. 2000), *aff'd sub nom.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001), on the ground that this characterization of "effective" would render the DMCA meaningless. Evidence of circumvention would demonstrate that the technological measure was not "effective," thereby legalizing the circumvention. The court was wrong not to recognize a spectrum of effectiveness, and wrong not to require proof by the plaintiff that its technology lay toward the strong end of that spectrum. *But see supra* note 46 (raising concerns about integration of technology and information content).

[343] *See* 18 U.S.C. § 1030(a)(2), (a)(5) (2000).

[344] 318 F.3d 58, 63 (1st Cir. 2003).

skipped the question almost entirely, focusing instead on the scope of authorized access. In *Register.com, Inc. v. Verio, Inc.*, the court inferred the defendant's lack of authority from non-binding Terms of Service posted on the plaintiff's Web site, thus importing into the CFAA the weakness of pre-*Specht* click-through law, and from the fact that the lawsuit was brought, thus importing an equivalent weakness from trespass doctrine.[345] In *EF Cultural Travel BV v. Explorica, Inc.*, the court inferred lack of authority from a nondisclosure agreement between the plaintiff and its former employee, one of the defendants.[346] Such an agreement might, in some circumstances, be considered sufficient warning of a potential access violation, so long as the subject matter identified in the agreement in fact encompassed the "confidential" information that is the subject of the CFAA claim. In *Explorica*, the agreement in question did not specify that information.[347]

One could imagine amending the CFAA to impose a sort of mens rea requirement for civil claims and thereby curing ambiguities regarding "knowledge" and "intent."[348] An amendment ought not to be necessary, if courts take seriously the requirement that a CFAA defendant's access be "without authorization" or have "exceeded authorized access."[349] In practical terms, this involves shifting a burden. As courts now interpret the authority requirement, so little evidence of absent authority will suffice that, in effect, authority is absent unless affirmatively granted by the information proprietor.[350] Nothing in the

---

[345] *See* 126 F. Supp. 2d 238, 249 (S.D.N.Y. 2000).

[346] *See* 274 F.3d 577, 582 (1st Cir. 2001).

[347] *See id.*

[348] Civil liability might even be eliminated altogether, although that prospect seems remote. Alternatively, one might imagine raising a "vagueness" objection to all or part of the statute. Such objections to the CFAA and to state criminal anti-hacking statutes have generally been rejected. Decisions rejecting vagueness arguments include *United States v. Fernandez*, No. 92 CR 563 (RO), 1993 WL 88197 (S.D.N.Y. Mar. 25, 1993); *People v. Hawkins*, 121 Cal. Rptr. 2d 627 (Ct. App. 2002); *Commonwealth v. Farley*, No. 95934, 1996 WL 1186936 (Mass. Super. Ct. Oct. 18, 1996); *State v. Washington*, 710 N.E. 2d 307 (Ohio Ct. App. 1998); and *State v. Johnson*, No. 59190, 1992 WL 25312 (Ohio Ct. App. Feb. 13, 1992). Vagueness arguments have been accepted in *Commonwealth v. Cocke*, 58 S.W. 3d 891 (Ky. Ct. App. 2001), and *State v. Azar*, 539 So. 2d 1222 (La. 1989).

[349] The CFAA defines "exceeds authorized access" in circular terms: "[T]he term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6) (2000).

[350] *See* United States v. Morris, 928 F.2d 504, 510–11 (2d Cir. 1991) (finding, in a criminal CFAA case, that intent requirement was satisfied by intentional access to computers beyond scope of authority, despite defendant's authority to access other computers on the network); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000) (concluding under common-law agency principles that

statute requires this result.[351] Implementing the foreseeability standard involves first shifting the burden of proof regarding the lack of authority to the plaintiff, and then requiring meaningful evidence of absent authority (such as an acknowledged click-through agreement, actual pre-access knowledge of the plaintiff's interest, or an effective technological measure limiting access) from the plaintiff. As in the discussions of click-through and trespass cases above, however, that evidence should not go solely to the defendant's knowledge, but instead to the understanding of the group of users of which the defendant is a member. *Zefer* does not represent the correct approach.

B. *Objections and Limitations*

1. Problems Not Solved

I have argued that courts mistakenly rely on the Internet-as-place metaphor to permit information proprietors to restrict access to computer facilities based on protected interests in those facilities, whereas in practice these plaintiffs are concerned with access to information itself. A foreseeability standard that implements a robust metaphorical sense of place allows those parties a sophisticated tool for self-protection with respect to both physical and information resources. The solution, in short, appears not to address one of the key weaknesses of the Internet-as-place metaphor—that it permits courts to obscure important distinctions between interests in tangible property and interests in intangible property. The analysis focuses, in other words, on assuring that use of metaphors is accurate, without addressing whether the results that would follow from its recommendations are correct.

Operation of the foreseeability standard on the physical characteristics of the information environment should not be read as foreclosing concern for virtual characteristics. Yet direct, boundary-based regulation of the electronic intangibles themselves is expensive,[352] frustrating,[353] or (sometimes, and) ineffective.[354] Regulation that fo-

---

employees lost authority to access computer system after acquiring interest adverse to employer).

[351] *See* 18 U.S.C. § 1030.

[352] Preemption and misuse arguments, for example, are litigated as defenses to claims of infringement brought by information proprietors.

[353] Frustrating is a term that aptly characterizes both efforts to enact UCITA (and before it, Article 2B of the UCC) as a uniform law of software licensing and to encourage reliance on enacted federal and uniform state statutes approving the use of electronic

cuses on the physical as a proxy for the virtual attempts to restore some of the regulatory benefits that tangibility once provided. Nothing in the proposal forecloses resort to information-specific doctrines such as federal preemption[355] of rights available under state law, or misuse of copyright or patent rights,[356] or the first sale doctrine in copyright law, for example.[357] The point of the proposal is to make application of those doctrines less subject to ambiguity caused by failures to distinguish between tangible and intangible interests. The standard does not necessarily solve all of the problems created by click-through cases, trespass to chattels, the DMCA, and the CFAA. Particularized applications of the standard in the context of each doctrine remain to be worked out, and additional regulation of access to information (distinguished from access to information storage) may be appropriate in each case.

---

signatures in commercial transactions. *See* UNIFORM ELECTRONIC TRANSACTIONS ACT OF 1999, *available at* http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm; Electronic Signatures in Global and National Commerce Act (ESIGN), *see also* 15 U.S.C. §§ 7001–7006, 7021 (2000). The former has been mired in controversy for years. The latter have been largely ignored.

[354] *Compare* Gordon, *supra* note 291, at 1380–84 (arguing that modern copyright's virtual boundaries serve as a proxy for older protections offered by limits of tangible copies of works), *with* Diane Leenheer Zimmerman, *Fitting Publicity Rights into Intellectual Property and Free Speech Theory: Sam, You Made the Pants Too Long!*, 10 DEPAUL-LCA J. ART & ENT. L. & POL'Y 283, 289 n.15 (2000) ("[A]s a practical matter, legislation, international trade agreements and even judicial decisions have chosen to ignore those theoretical boundaries to an extent that makes it difficult for me to state that they continue to have any real life left in them.").

[355] *See, e.g.*, 17 U.S.C. § 301 (2000).

[356] The proposal in the text encourages the development of boundaries or other points of visibility or salience in cyberspace, but nothing mandates that those boundaries be established, initially, in their proper places. In cases of overreaching, public policy should step in. Preemption of state contract law by federal copyright law, for example, plays an important role in maintaining boundaries within appropriate limits. *But see* Bowers v. Baystate Technologies, Inc., 320 F.3d 1317, 1325–26 (Fed. Cir. 2003) (holding that shrinkwrap agreement barring reverse engineering of computer program may be enforced notwithstanding conflict with copyright law). Different access doctrines might preempt one another. *See* Hardy, *supra* note 140, ¶¶ 10, 13 (both suggesting that trespass-to-chattels claims may be preempted by copyright law to the extent that they address copying of information); O'Rourke, *supra* note 41, at 590. Public policy limitations may be supplied by sources beyond intellectual property law. *See* People v. Network Assocs., Inc., No. 400590/02, slip op. at 6–9 (N.Y. Sup. Ct. Jan. 14, 2003), *available at* http://www.eff.org/IP/UCITA_UCC2B/spitzer-v-network-assic.pdf (enjoining enforcement of license term prohibiting unauthorized reviews of computer program because license terms represented deceptive acts in the conduct of business). For a compelling argument supporting extension of misuse principles to the DMCA, see generally Burk, *supra* note 212.

[357] *See* 17 U.S.C. § 109(a).

2. Negative External Effects

The foreseeability standard encourages use of more robust technical and other barriers to access to information. To that extent, the standard is associated with the negative consumer-related externalities associated generally with reliance on private contract and related measures used to limit access to information. In economic terms, consumer benefits from information access exist partly because of mandatory rules preserving such access, and partly because information proprietors do not have the benefit of rules that state precisely when they may legally limit such access.[358] Application of the former principle can be addressed by the argument presented in the preceding section, because the foreseeability standard should increase the effectiveness of mandatory information access principles.

The second point, that external benefits from information production and consumption arise because of fuzziness in the law, raises an important issue if one assumes that the inevitable tendency of the world of information proprietors is to increase barriers to information access.[359] As a practical matter, it is difficult to conceive of a world of information production in which information proprietors have more incentives to privatize their works than they do currently. At worst, the level of private efforts to limit access would remain constant, and both the effectiveness of such efforts and their cost to information proprietors would increase. It is difficult to see how information users would be made worse off. By contrast, the need for alternative strategies to regulate access, and for the ability to apply those strategies effectively, would become clearer.

The shift to a foreseeability standard and any corresponding increase in the costs associated with proprietors' efforts to limit access might also lead to more measured use of access restrictions and to corresponding consumer benefits. The foreseeability standard is intended to reinforce the notion of salience of limits on access, rather

---

[358] *See* Julie E. Cohen, *Copyright and the Perfect Curve*, 53 VAND. L. REV. 1799, 1807–08 (2000); William W. Fisher III, *Property and Contract on the Internet*, 73 CHI.-KENT L. REV. 1203, 1240–46 (1998); Michael J. Madison, *Complexity and Copyright in Contradiction*, 18 CARDOZO ARTS & ENT. L.J. 125, 140–44 (2000).

[359] More abstractly, it is possible that the argument does not give sufficient credit to the risk of anticommons. A property regime that permits maintenance of too many boundaries runs the risk of stifling innovation and development, rather than encouraging it through appropriate management of privatization incentives. *See generally* Michael A. Heller, *The Tragedy of the Anticommons: Property in the Transition from Marx to Markets*, 111 HARV. L. REV. 621 (1998).

than to give information proprietors more effective ammunition in arguing for their existence. Imageability in urban planning supposes not that every street serves as a barrier, but that some physical features are salient in a given landscape and are therefore deserving of special recognition in the planning calculus.[360] Some are salient because of their privatizing characteristics.[361] Others are salient because of their role in constructing or defining public space.[362] In either case, imageability is costly, both economically and cognitively. Not every apparent landmark counts. By analogy, not every boundary can be an effective access control. It has been observed more generally that the social harms caused by expansive rights in information can best be limited by clearly defining the scope of those rights, via legal doctrine if possible, and via mechanical restraint if need be.[363]

3. The End-to-End Principle and The Dynamic Internet

The essence of the Internet, if it has an essence, lies in the technology of openness that underlies it and the culture of openness that the technology facilitates and signifies. The argument from openness suggests that both structure and culture lead to worthwhile innovation and invention that would otherwise be limited by "traditional," or controlled, information production and distribution systems.[364] Innovation is supported technically because, as a default matter, the Internet does not preclude users from experimenting with its capabilities. The technical infrastructure of the Internet relies on a core principle

---

[360] *See supra* notes 274–285 and accompanying text.

[361] *See supra* notes 274–285 and accompanying text.

[362] *See supra* notes 274–285 and accompanying text.

[363] Wendy Gordon has made this argument in the context of copyright law. *See* Wendy J. Gordon, *A Property Right in Self-Expression: Equality and Individualism in the Natural Law of Intellectual Property*, 102 YALE L.J. 1533, 1606–08 (1993); *see also* Timothy P. Terrell & Jane S. Smith, *Publicity, Liberty, and Intellectual Property: A Conceptual and Economic Analysis of the Inheritability Issue*, 34 EMORY L.J. 1, 28–32 (1985) (arguing that property rights in general can be understood as manifestations of "thingness" or "specificity"). More abstractly, mere "zoning" of the Internet should ordinarily be insufficient to satisfy the foreseeability standard. *See* Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 883–95 (1996) (observing that the Internet is capable of and is in fact being "zoned"); *see also* Reno v. ACLU, 521 U.S. 844, 890 (1997) (O'Connor, J., concurring in part and dissenting in part) (relying on Professor Lessig's work to suggest that zoning of the Internet is desirable and, by extending principles guiding zoning of real property, possible).

[364] *See* Lawrence Lessig, *The Architecture of Innovation*, 51 DUKE L.J. 1783, 1790–91 (2002).

of "end-to-end" connectivity.[365] Other things being equal, network traffic should encounter interpretive activity (discrimination based on its content) at the "ends" of the network, or at user nodes, rather than at locations closer to its core.[366] Networked electronic information should be distinguished and interpreted by different end-user software applications, for example, rather than by firewall software. A legal perspective that rewards information proprietors who build strong boundaries on the Internet appears to interfere both technically and culturally with these frameworks for innovation.

The foreseeability standard need not conflict with the end-to-end principle, if that principle is accepted as a guiding public policy. Visible barriers to access can be implemented in any number of ways, many if not most of them manifested at or near the application level.[367] Generally, and for the reasons described in the preceding section, the foreseeability standard should be understood not as an impediment to innovation and invention, but as a measured attempt to protect the Internet as a field of innovation from encroachment by the Internet-as-place metaphor interpreted in absolute terms. It is possible that the world of information would be a better place if there were no boundaries or barriers anywhere on the Internet. Such a world is not among the choices we face. The policy and legal choice is not between a world of no boundaries and a world of measured boundaries. It is between a world of measured boundaries and a world of absolute boundaries, where all access comes at a price, measured either *ex ante* or (increasingly, and without warning) *ex post*.[368] Being able to see the shape of the Internet ought to be a relatively small price to pay in exchange for the former.

Conclusion

The dominant metaphor governing discussion and legal analysis of information-related problems on the Internet can be translated

---

[365] The origins of the principle as a technical guideline for systems development, and its application to Internet policy, are reviewed in Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. Rev. 925, 930–33 (2001).

[366] *Id.*

[367] *See* Timothy Wu, *Application-Centered Internet Analysis*, 85 Va. L. Rev. 1163, 1184–88 (1999).

[368] This concern with *ex post* rather than *ex ante* regulation mirrors that expressed by critics of the electronic self-help provision found in an earlier version of UCITA. *See* Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 Berkeley Tech. L.J. 1089, 1115–18 (1998).

into legal doctrine in ways that address both producer and consumer interests in access to information. That translation can be accomplished by linking our metaphorical appreciation of place to our common experience of physical place. There are some important assumptions built into that link, assumptions that are unprovable but are based on observation and experience. Our language and our experience share cognitive sources. The meaning of our metaphors remains essentially constant across context. And both metaphor and experience do and therefore should guide legal analysis. I argue that our common experience (i.e., that places are freely accessible when they appear to be so, and that landmarks and boundaries of various sorts signal the existence of limits) is relevant to what we mean by place metaphors, and that both that experience and that meaning ought to be carried over not only to our experience of electronic place but also to our legal analysis of electronic place. The burden of exclusion from information ought to fall more concretely on the information proprietor on the Internet—as it does, in practice, in the tangible world. A unifying standard, foreseeability, can be abstracted from that proposition and interpreted in the context of legal doctrines of contract, trespass, the DMCA, and the CFAA, now used to regulate access to information. Idiosyncratic issues would remain to be worked out in the context of each doctrine, and in the context of others used for the same purpose. Those idiosyncrasies should not obscure the fact that what we face presently is an unrecognized and inconsistent law of access to electronic information. The approach presented here represents a start towards making sense of that law.