Poisoned Flowers in Cyberspace: Resolving Focal Point Abuses and Trademark-Related Conflicts in Space by Rewriting Code

Thomas C. Folsom, Regent University
POISONED FLOWERS IN CYBERSPACE:
RESOLVING FOCAL POINT ABUSES AND TRADEMARK-RELATED CONFLICTS IN SPACE BY REWRITING CODE

Thomas C. Folsom

Okay . . . why not make the petals poisonous only when in the possession of someone who purchased them? If they are stolen, or if they blow away, then let the petals lose their poison.

ABSTRACT

In cyberspace, dynamically coded focal points don’t just provide salient references. They can actually deliver a person’s augmented presence to a location. Placing reliable focal points as navigational markers in coded space is useful and indexing them is even better because these activities support the public good by providing a virtual map to cyberspace, thereby promoting access, navigation, information-activity and trust among augmented presences. In an objective cyberspace which relies upon a virtual map featuring dynamically coded focal points functioning as markers, addresses, magnets, roadblocks or detours, I propose that conduct which (a) alters the virtual map, (b) plants deceptive focal points, (c) ambushes a user of focal points with uninvited or false invitations, or (d) expropriates, blocks or spoils focal points otherwise available, should be an actionable focal point offense. The focal point offense can be specified and is limited by a “common remedy” purposely designed to be flexible, proportionate and graduated to promote a modest recoding of cyberspace to preserve its foundational values. Upon request, the common remedy forces a reasonable technological accommodation by some combination of effective (1) disclaimer, (2) notice, (3) forced redirect/release, (4) reciprocal auction, or (5) opt-out/opt-in. This avoids the all-or-nothing prohibitory remedies attending current trademark infringement, cybersquatting, uniform domain name dispute resolutions, and similar patchwork solutions to mark-type disputes in cyberspace. The common remedy disarms the poisonous nature of the flowers planted in the code world, but also preserves a thriving, robust and dynamic cyberspace. I propose a comprehensive and coherent method of designing law for the code world of which

* © Thomas C. Folsom 2009.
** Professor, Regent University School of Law; J.D., Georgetown University Law Center; B.S., United States Air Force Academy. I thank the International Trademark Association (INTA) for permitting me to present a version of the first section of this article in May, 2009 in Seattle at their 131st Annual Meeting and I am especially grateful to Jeremy Phillips, moderator of the INTA panel, for his generous support of the concept. I thank the Intellectual Property Scholars’ Conference for permitting me to present a modified version of the first section of this article in August, 2009 at the Cardozo Law School in New York at their 9th Annual Conference, and I thank Dean Toben and Professors Swenson, Osler and Powell for inviting me to present a version in October, 2009 at the Baylor University Law School. I am also grateful to INTA for awarding me the 2009 Ladas Memorial Award for writing excellence on the subject of trademarks and related matters for my article, Space Pirates, Hitchhikers, Guides and the Public Interest: Transformational Trademark Law in Cyberspace. This article is, in effect, the second part of the Space Pirates piece delayed only because of lack of time and space, and it now completes the arguments there begun. My Research Assistants this year have been Shannon Brown, Nathan Hall, Nicholas Lepire, Jonathan McDowell and Andrew Page, and I thank each of them. Joanne Kelvington has continued to provide invaluable editorial and research support as a Research Assistant, emeritus. The errors are mine.

1 LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999).
cyberspace is a part.

All focal point offenses use expressions functioning as markers or spoilers in cyberspace, and some of the more effective focal points incorporate trademarks. Quite apart from trademark-related law, I claim the specified focal point offenses in cyberspace constitute independently actionable misrepresentation or deceit, misappropriation or theft, spoilage or unfair competition. While some focal point offenses might also constitute trademark infringement, it is not immediately helpful to try to resolve all focal point offenses in cyberspace by “ordinary” principles of trademark law as developed in ordinary space. Trademark law as currently misapplied to focal point conflicts in cyberspace has raised curiously novel defenses and other aberrations that more frequently obscure than reveal what is happening in cyberspace while defacing trademark law itself. Current trademark likelihood of confusion factors, even when carefully applied, are not able reliably to predict a “likelihood of confusion” by attenuated or invisible uses of trademarked expressions in cyberspace, much less resolve the real problems caused by focal point offenses. If there is to be a likelihood of confusion analysis for some residual cases in which the proprietor might desire to assert trademark liability in addition to asserting a focal point offense, I propose a new factor to determine trademark likelihood of confusion by a rationally demonstrable “nature and place of use” analysis.

This Article extends an argument begun in a series of prior Articles and is intended to persuade juridical actors actually to adopt the proposed new solution. I claim the new approach does three things: (1) it works—it provides a highly practical resolution of cyberspace focal point conflicts because it more reliably gets to the correct result, for the right reason, persuasively explained than any other proposed solution, (2) it is efficient—it allocates costs and benefits among cyberspace actors in a Pareto-optimal manner, and (3) it is authorized, predictable and principled—it is recognizably derived from existing patterns of law already regulating misrepresentation, misappropriation, and unfair competition, and can easily coexist with trademark-related law. I also claim it is better in all three respects than any other competing explanation of, or proposal for how to deal with invisible or attenuated trademark conflicts in cyberspace.

TABLE OF CONTENTS

Introduction ........................................................................................................................6
I. The Focal Point Offense: It Can Be Specified .................................................................8
   A. Terminology: Framing the Issue ............................................................................9
   B. The Specified Offense ....................................................................................22
   C. Summary ........................................................................................................34
II. Applying the New Solution: It Works ...........................................................................36
   A. Illustrations ....................................................................................................41
   B. Cases ............................................................................................................60
   C. Avoiding Spectacular Error ............................................................................68
III. Counting the Costs of the New Factor: It Is Efficient ..................................................69
   A. Reallocating Burdens among Cyberspace Actors ............................................71
   B. New Institutional Economics: Accounting for Juridical Agency Costs ..........85
Deliberate deceit, theft or spoilage accomplished by the offensive use of focal points in cyberspace does not suddenly become privileged conduct just because the offender also incorporates someone else’s trademark and ingeniously claims she is not “using” the focal point “as” a trademark, but merely as a fraudulent marker or as an expropriating spoiler. Conversely, value-adding conduct in cyberspace including technologically reasonable accommodations to mitigate any incidental harm should not be forbidden simply because a trademark is somehow involved in a focal point creating some “initial interest” in something somewhere in cyberspace (that is, of course, precisely what a legitimate navigational focal point is supposed to do, else it wouldn’t be a focal point at all).

The ability simply to change the code, and thereby alter the objective reality of cyberspace, is a feature remarked upon by Professor Lessig. He poses the striking hypothetical of the poisonous-flower-that-kills-the-neighbor’s-dog and then easily resolves the conflict between neighbors by a reasonable technological accommodation: upon request and after a short conversation, the offending party simply rewrites the code to change the properties of the poisonous flowers, and in a Pareto superior move to boot. Of course, Professor Lessig’s story occurs in a

---

2 Id. passim.

3 The hypothetical begins as follows: “Martha grew flowers. Not just any flowers, but flowers with an odd sort of power. They were beautiful flowers, and their scent entranced. But however beautiful, these flowers were also poisonous. For this was Martha’s weird idea: to make flowers of extraordinary beauty which, if touched, would kill…” Id. at 9-10. Compare the Oleander (Nerium oleander) which is said to be “one of the most poisonous plants in the world” but whose “leaves, flowers and fruit contain cardiac glycosides, which … are likely to send someone into cardiac arrest should he eat part of the plant… People tend to be blasé, because the flowers are bright and pretty, sort of candy-colored. But it is a very poisonous plant that will stop your heart.” Chris Sweeney, Top 10 Most Dangerous Plants in the World, POPULAR MECHANICS, Sep. 16, 2009, http://www.popularmechanics.com/science/earth/ (emphasis added) (last visited, Sep. 19, 2009) (source suggested by Professor Glenn Reynolds at Instapundit.com).

4 The hypothetical’s conflict concerns a dead dog. Id. According to the hypothetical, two neighbors, Martha and Dank, are at odds. Dank’s dog is dead. It is dead because it ate the petals of Martha’s poisonous flowers borne on the wind from Martha’s land to Dank’s. Martha made the flowers poisonous on purpose. She sells them to a select clientele who value them highly because of the tantalizing combination of beauty coupled with the risk of death. As Professor Lessig soon reveals, the conflict arising out of the poisonous flowers occurs in cyberspace, in which both the flowers and other things are constructs created by code, having properties determined by code.

5 Id. at 12-13. The hypothetical negotiation between the neighbors is short and to the point. Martha first suggests that Dank simply “make” a new dog that won’t die. Dank counters that Martha should make her flowers lose their poison when they leave her property. Because the commercial value of the flowers is precisely that she intends to sell some of them (and to hold their value, they must retain their poisonous character after leaving her property), she won’t accept that proposal. Yet they soon hit upon the sensible expedient upon which both can agree: she will remake her flowers so that they lose their poison if they leave her property without her consent. In short order, the conflict is resolved to everyone’s satisfaction, and at essentially no cost, other than some slight
coded world which is regulated or influenced by a combination of laws, markets, norms and architecture.\footnote{5}

I claim that if the legal influencers on conduct could be made to coincide with the other factors which influence conduct, and in a way supporting the foundational values of cyberspace, then it is much more likely the offending party might actually “volunteer” to rewrite the code upon request than if the law exonerated the offending conduct altogether, as it might do if juridical actors woodenly applied the law of ordinary space to all aspects of the code world.\footnote{7} I am concerned about the case in which Martha, or any other owner of the flowers, might say to the owner of the dead dog something to this effect: “No. You can’t make me. I will not recode nor will I do anything else to help you.”\footnote{8} Norms having failed to influence the desired response from the offending party,\footnote{9} this response transaction costs (it being assumed that Martha either knows how to write code, or that she can find someone else to do so, it being further assumed that there is just a line or two of code to change in some structured, object-oriented programming environment and that the change would not constitute any unprivileged infringement of any copyright held by some other author of the underlying code, and so all this constitutes a technologically reasonable accommodation by Martha to Dank). See id. By the way, this solution is not only Pareto superior but absolutely superior simply from Martha’s perspective alone (it protects her own stock in trade from thieves as well as from innocent finders of the wind-borne inventory who might subsequently compete by reselling the found goods).

See id. at e.g. Chapter 7, pp. 85-99 (describing four things that regulate or influence conduct: laws, norms, markets and architecture). \textit{Id.}, Appendix at 235-39 (extending the argument). One could add associations and virtues to the list of influencers, but the point remains: law is but one influencer and architecture or code is another. If the two could be made more nearly congruent, they would become more nearly complementary to each other, and if they were designed with some deliberate choice in mind, they might more nearly embody the choice of an explicitly considered and desirable architecture than not.

Perhaps negligence, nuisance, or some other law might provide, or might be stretched to provide redress, but the transaction costs are higher, the uncertainty greater, and the stress placed upon the ordinary law more severe than if she had simply recoded her offending flowers in cyberspace.

See supra note 5. I think we can assume the idyllic, rationally beneficent resolution offered by Professor Lessig certainly occurs from time to time, but not all the time. If such an attitude as displayed by his hypothetical characters were universal, we wouldn’t need laws. The problem for law resides in precisely the set of cases in which someone in Martha’s position refuses. Because our current laws applicable to cyberspace have utterly no principled or predictable ability to compel Martha’s consent, our current laws are utterly useless to the task of “choosing” a rationally beneficent solution, notwithstanding the fact that the architecture of the code world makes such a choice cheap, easy, and fast. An equally serious problem is the worry that, once the “ordinary” law of, say, nuisance is modified to force Martha’s hand in the code world, then those principles might well be cited in ordinary space radically distorting (or at least changing) the balance in the ordinary law. My proposal avoids the problems of doctrinal creep and unintended feedback loops by localizing the new solution in relation to the place of use; it is explicitly a law for cyberspace.

\footnote{5} Cf. generally, e.g., Jacqueline D. Lipton, \textit{Bad Faith in Cyberspace: Grounding Domain Name Theory in Trademark, Property and Restitution, forthcoming}, HARV. J.L. & TECH. (preliminary copy available at SSRN, last viewed on December 19, 2009) (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1484763) (discussing norms generated by the concept of bad faith); Dotan Oliar and Christopher Jon Sprigman, \textit{There’s No Free Laugh (Anymore): The Emergence of Intellectual Property Norms and the Transformation of Stand-Up Comedy}, 94 Va. L.REV. ___ (2008) (discussing norms generated by the community of comedians); Graeme B. Dinwoodie, \textit{Private Ordering and the Creation of International Copyright Norms: The role of Public Structuring}, 1 J. INST’n. & THEORETICAL ECON. 160 (2004) (discussing norms generated by Internet Service Providers and by digital rights management systems). Of course, if humankind were composed of [good] angels who therefore invariably followed normative virtues then, as the argument went, we wouldn’t need any laws at all. See \textit{The FEDERALIST} No. 51, at 163 (James Madison) (Encyclopedia Britannica ed. 1952) (asserting that if men were angels no “government” would be necessary). It is because persons are, in fact, not angels much less good angels and norms fail or flag that we should at least consider whether and if so how some law might help by encouraging some rationally desirable norm in cyberspace, such as the norm of recoding according to a “\textit{sic utere tuo ut alienam non laedas}” principle (so that Martha might “so use her own” coded flowers “as not to disturb” Dank’s coded dog as by killing it, especially when Martha may do so at essentially no cost).

\footnote{7} Perhaps negligence, nuisance, or some other law might provide, or might be stretched to provide redress, but the transaction costs are higher, the uncertainty greater, and the stress placed upon the ordinary law more severe than if she had simply recoded her offending flowers in cyberspace.

\footnote{8} Perhaps negligence, nuisance, or some other law might provide, or might be stretched to provide redress, but the transaction costs are higher, the uncertainty greater, and the stress placed upon the ordinary law more severe than if she had simply recoded her offending flowers in cyberspace.

\footnote{9} Perhaps negligence, nuisance, or some other law might provide, or might be stretched to provide redress, but the transaction costs are higher, the uncertainty greater, and the stress placed upon the ordinary law more severe than if she had simply recoded her offending flowers in cyberspace.
would throw the offended party back upon “ordinary” law for recourse.\textsuperscript{10} Instead of distorting ordinary law to accommodate the unusual, extraordinary characteristics of the code world, it is my claim that a transformed law for the code world can provide a surprisingly easy rule of thumb which is modular and self-contained (fitted and confined to the code world).

After several decades of experience with the code world, cyberspace, new machines, new users and new technological uses (NTUs) within that world, it is long past time to take off the training wheels and to stop pretending we are still stuck in the twentieth century. It is time actually to start choosing solutions and resolving the characteristic problems of cyberspace. What, indeed, will we do with poisonous flowers\textsuperscript{11} in cyberspace? What do we do if the owner, creator or distributor of the flowers simply says “no, I will not, and there is nothing you can do about it”? It can scarcely be emphasized enough that the poisonous flower in cyberspace is no metaphor at all, but real.\textsuperscript{12} The poisonous flower hypothetical is an example, not of some figure of speech applicable to cyberspace, but of the different reality existing in the code world and cyberspace compared to the reality existing in “ordinary” space.

This Article is part of a larger project to specify and to design contemporary legal solutions based on a common morality for a global/tech age. This Article concerns the tech side of the project and so it will share some of the features of the coded world it describes.\textsuperscript{13} It is a coded world, after all, that the law is seeking to

\footnotesize{\textsuperscript{10} I am not yet urging that there be a law “of” cyberspace, but merely a law that is suitable “for” cyberspace. The well-known problems of doctrinal creep, reverse doctrinal creep, lateral doctrinal creep and feedback loops are, in fact, avoided only when there is a law suitable “for” the particular real relationships and actual characteristics involved in the recurring disputes that actually occur in cyberspace: not a law “of” some over-generalized, fossilized, totemic and ill-adroit wooden application of old doctrines where they manifestly don’t fit. In some plurality (maybe a majority) of cases, cyberspace conflicts might present merely a routine transposition of a transaction common to ordinary space. No special accommodation is needed for such. But in other cases, cyberspace conflicts actually are, not to mince words, “essentially” different from any in ordinary space because the code world actually “does” things that ordinary space cannot comprehend. For such cases, a law suitable “for” cyberspace would seem rather obviously desirable. See section infra.

\textsuperscript{11} Flowers have long provided powerful grounds for metaphor, yet even the force of the metaphor changes depending on whether we are dealing with the coded world of cyberspace or the more constrained world of “ordinary” space in which we cannot so easily rewrite code to change the consequences. Compare, e.g., MATTHEW 6:28 (“Consider the lilies of the field, how they grow. . .”) (pointing to characteristics of flowers in ordinary space, not coded into them by any of us who perceive them); CHARLES BEAUDELAIRE, LES FLEURS DU MAL (1857) (pointing, by metaphor, to dangerous flowers whose consequences linger and cannot easily be coded or wished away); Lu Ting-yi, “Let Flowers of Many Kinds Blossom” Speech Delivered May 26, 1956 (often attributed to Mao Tse-tung and rendered as “let a thousand flowers bloom”) (pointing to many flowers, but manifesting a contradiction in an invitation to free expression which is also dangerously unconfined since not every metaphorical flower is permissible and some are deemed counter-revolutionary: “and for them we have only dictatorship”). But all metaphors aside, the question remains: what will we do with flowers in an objective cyberspace that we actually can code, recode or otherwise change?

\textsuperscript{12} In an objective cyberspace in which code can be perceived, reproduced or otherwise communicated either directly or indirectly by way of a machine or device, the coded objects can leave an objective trace, and can cause observable (real) effects. That which causes a real effect must itself be real, and so is code.

\textsuperscript{13} It is built in a step-wise modular fashion and it tends, moreover, to call previously written methods, but with modest repetition so the argument will work regardless where the reader chooses to enter. With apologies to Professor Cooper, I’ve received much advice on this manuscript, “including suggestions that it be longer, shorter, harder, easier, funnier yet more serious, with fewer and additional [examples, cases, illustrations] and problems that are simpler and more difficult to do, as well as more but less [technologically] oriented.” DOUG COOPER & MICHAEL CLANCY, OH! PASCAL!, xiii (2nd. ed. 1992). I hope to have produced “a presentation that’s detailed enough for [experts], yet lucid, readable, and enjoyable enough for [interested non-experts] to read…” Id at xv. As the good professor declares: “if YouCanReadThis then begin”. Id. at xxi.}
regulate, and in “holding the mirror up” to this coded “nature” it is well to remember, first, that any mirror image is reversed, and second, that real things in the code world sometimes work pretty much like the way things work in the ordinary world, but sometimes in ways that are different and which make a difference.  

INTRODUCTION

Part I of this Article sets up a preliminary condition, and the first test: can the focal point offense be stated in rule-specific form? I claim it can. Moreover, I claim that the same general factor for the development of normative legal rules anywhere in the code world, “the nature and place of use,” can not only regulate focal point conflicts in cyberspace, including those which incorporate trademarks, but can thereby also comprehensively regulate all mark-related conflicts there. By way of example, the same general approach can also, with sensible variations, be re-specified as a new “likelihood of confusion” factor more rationally to assess trademark infringement by invisible and attenuated uses in space. Coupled with a common remedy for common offenses, the new approach can integrate the proposed focal point offense with all the residual instances in which it might still be appropriate to invoke any of the existing laws and other authorities which currently attempt to regulate mark-type conflicts in cyberspace. The integration of the current crazy-quilt into a comprehensive and coherent whole is an additional benefit of my approach.

Part II of this Article presents a second test of the new approach: does it work? If the fully specified new nature and place of use factor works better than competing approaches, it must be because, compared to current approaches, it is more likely to assist juridical agents in reaching the correct results, for the right reasons, persuasively explained. To pass the first test, the proposed focal point offense (and the complementary “nature and place of use” factor for trademark’s likelihood of confusion evaluation) must resolve actual cases while avoiding or dramatically minimizing the risk of spectacular error inherent in current approaches to the problem. This claim will be tested by applying the new analyses to illustrative hypothetical and already-decided cases, and by considering the cost of errors or misapplications of the new factor.

Part III of this Article presents a third test: does the proposed solution efficiently allocate the costs and benefits of focal points in cyberspace? I assert the proposed solution is efficient and affordable because its benefits outweigh the costs—each of the persons affected by the new factor is fairly burdened by the costs and benefits it provides. This assertion is tested by dividing the cyberspace actors and accounting at a rough level of approximation for the mix of anticipated

---

14 Compare WILLIAM SHAKESPEARE, HAMLET, Act III, sc. ii., ll. 17-24 (the purpose of “playing” is “to hold, as ’twere, the mirror up to nature”), with LEWIS CARROLL, THROUGH THE LOOKING GLASS AND WHAT ALICE FOUND THERE, 144 (reprinted in THE ANNOTATED ALICE (Martin Gardner ed., 2000)) (1897) (stepping through the mirror into a similar but different world, Alice “began looking about, and noticed that what could be seen from the old room was quite common and uninteresting, but that all the rest was as different as possible.” And cf., PAUL, 1 COR. 13:12 (warning that ordinary space itself is not entirely clear, “for now we see through a glass [mirror], darkly); RICHARD RORTY, PHILOSOPHY AND THE MIRROR OF NATURE (1979) (asserting that, perhaps in ordinary space there is nothing to see, or for a mirror to reflect).
benefits and burdens to each group affected by the new factor. When it comes to counting the costs, there are three constituencies or groups: (1) the primary users of cyberspace who cause or suffer the consequences of focal point and mark-type disputes; (2) the juridical actors who must negotiate, structure, resolve, regulate, teach or explain the results; and (3) the public whose perception of the rule of law is itself something worth considering.

Part IV of this Article presents a fourth test: can the focal point offense be implemented by common law judges and other juridical agents under existing statutes, norms and other governing authorities? I claim both the proposed focal point offense and also the new nature and place of use analysis for trademark’s likelihood of confusion are authorized and capable of principled application. The resolution of focal points in space relies upon recognizable principles of existing law, either as reasonably extended, or as reasonably transformed to respond to the real relationships and activities in cyberspace. The proposed cyberspace focal point offense constitutes a variety of actionable misrepresentation or deceit, misappropriation or theft, spoilage or unfair competition. When a trademark is involved, it might also constitute an independent act of trademark infringement.

This last claim is tested by explicitly considering certain trademark and related principles which cyberspace pushes to the breaking point. These include the trademark doctrines of initial interest confusion; an independent use “as” a mark requirement, if any; secondary liability; and more general trademark problems of doctrinal creep, reverse doctrinal creep, lateral doctrinal creep, equivocation, and the question-begging feedback loop in deciding new cases. It also considers cognate principles of unfair competition as applied to misappropriation, deceit and spoilage in space. Finally, I address problems of juridical authority and capability.

The Article concludes with a prospectus for further work. It seeks to enlist the support of practicing lawyers, judges and academics in a cooperative project that could be at once practical, principled and predictable. The project is to extend or transform recognizable principles of law to accommodate new machines and new technological uses in the code world, cyberspace, the metaverse, and ordinary space in a way that makes sense.

I should point out that this Article extends an argument begun in a series of prior Articles, including analytical, doctrinal, normative and other observations on designing laws for cyberspace. In my prior articles, I have claimed the preliminary task is to defend two propositions: that there “is” an objective cyberspace with defining characteristics suitable for positing a public

15 Thomas C. Folsom, Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality), 9 TULANE TECH. & IP LAW JOURNAL 75 (2007) [Defining Cyberspace].
17 Thomas C. Folsom, Space Pirates, Hitchhikers, Guides, and the Public Interest: Transformational Trademark Law in Cyberspace, 60 RUTGERS LAW REV. 825 (2008) [Space Pirates].
18 Thomas C. Folsom, Towards Non-Neutral First Principles of Private Law: Designing Secondary Liability Rules for New Technological Uses, 3 AKRON INTELL. PROP. J. 43 (2009) [Non-Neutral Principles]; and see generally, Thomas C. Folsom, Truth in Intellectual Property Revisited: Embracing eBay at the Edge, 2 AKRON INTELL. PROP. J. 69 (2008) (generalizing the public interest in limited remedies from patent law to copyright and trademark, and including those cases which involve asserted likelihood of confusion in respect of “invisible” trademarks) [Embracing eBay].
interest, and that it presents at least some important and recurring conflicts which current law is systemically unable to handle. This being so, the next level problem is actually to design a law more suitable for cyberspace and the code world. In the course of doing so it is necessary at the same time explicitly to reconsider remedies and principles of secondary liability as they relate to new technological uses in the code world.

In completing the solution to mark-type conflicts in space, I am here proposing a rather broad “focal point offense” in cyberspace, but I couple it with a tailored, narrow, proportionate and limited “common remedy” consisting of reasonable technological accommodations, applied on request. The complete solution also takes the problem of secondary liability into account by limiting the liability of targeted defendants who promote and embed technological accommodations within their coded systems. The desired solution for cyberspace must be, and my proposal is, comprehensive because each issue connects with many others. In this Article, I complete the full specification of the focal point offense and then address three practical questions: Does it work? Is it efficient? Is it authorized?

I. THE FOCAL POINT OFFENSE: IT CAN BE SPECIFIED

My threshold claim is that the focal point offense can be specified. I further claim the focal point solution works much more easily than any competing model, its benefits greatly exceed the costs of implementation, it is clearly permissible

---

19 I claim to have made that demonstration. Folsom, Defining Cyberspace, supra note 15.
20 I believe I have demonstrated this to be true, at least in the context of trademarks. Folsom, Missing the Mark, supra note 16. One sign of a systemic problem is when two lines of cases might each claim merely to be applying “ordinary” principles of trademark law to cyberspace and yet contradict each other while at the same time making strange innovations to trademark law as generally understood. Id.
21 I began this task by first specifying a trademark law suitable for special problems in cyberspace. Folsom, Space Pirates, supra note 17 (designing trademark likelihood of confusion factors suitable for invisible and attenuated uses in cyberspace). I claim to have developed a quick, easy, and practical rule of thumb (a heuristic) for handling such cases, removing the systemic juridical risk from the perspective of trademark-related law. This Article begins where Space Pirates left off and I am now explicitly supplying the larger context, folding the transformed likelihood of confusion factors into the broader, quicker, easier, and more practical focal point offense. This Article completes the task of specifying a transformed trademark-related law for cyberspace which was begun in Space Pirates.
22 Folsom, Embracing eBay, supra note 18.
23 Folsom, Non-Neutral Principles, supra note 18.
24 See infra, Sections I.B.1 (the focal point offence) & I.B. 4 (the common remedy). Beyond this, I speak of a new “nature and place of use” likelihood of confusion factor for residual cases of trademark infringement, but coupled to the same proportionate and limited “common remedy” so long as the offense arises out of an “invisible and attenuated” use of a mark within a focal point. See infra, Sections I.B.5 (integrating trademark likelihood of confusion and related laws). I also deal with potential secondary liability. Without these and similar connections, the various pieces do not work well.
25 I am posing three practical problems beyond those previously addressed. All of the connections necessary to the arguments made herein will be supplied in this Article. I reference the prior articles not to suggest that any reader of this one need to read any or all of those, but merely to point out that the reader may find in them a more complete treatment of some issues only briefly treated herein. My citations to myself will not be exhaustive, nor will I always indicate when I quote myself. Instead, many of my self-referencing footnotes are simply to alert the reader that there might be a more substantial treatment elsewhere. For ease of reference, I have digested many of the prior points into the form of an Appendix A and an Appendix B attached hereto. A reader might think of these related articles as forming, at least in the author’s mind, a book in serial form: I think of my self-citations as if to earlier chapters in the same book, but for the reader’s convenience I have endeavored to keep each chapter (each Article) sufficiently self-contained that it may be read on its own terms. Cf. RICHARD A. POSNER, THE LITTLE BOOK OF PLAGIARISM, 64-65 (2007) (exonerating, perhaps, some self-plagiarism in the interest of developing, refining, and expanding the reach of somewhat novel ideas).
under existing principles of law, and it ought to be adopted. But this first section simply explains the threshold claim. I summarize the new focal point offense in rule-specific form, relating it to a specified nature and place of use factor for trademark’s likelihood of confusion analysis, coupled with a common and limited remedy. The initial “cost” of adopting the new approach is the time and effort of understanding it and the preliminary test condition is actually to state the offense in a rule-specific form.

The new approach is disarmingly simple and easy, but like all truly simple paradigm-shifting solutions, it takes some effort to explain how simple it is and why the existing approaches are, notwithstanding their familiarity, needlessly complicated by disconcerting anomalies and in need of replacement. This first Section is in three parts: Part A introduces terminology and frames the issues in three sub-sections. Part B sets forth the specified offense in five sub-sections. Part C provides a summary of the specified offense in the context of other mark-related rules.

A. Terminology: Framing the Issue

This Part sets the scene in three subsections. First, I introduce my key terms: focal points, markers and spoilers. Next, I map these terms to more traditional trademark concerns and assert that they isolate a failure in trademark law. Finally, I provide a brief outline of the solution.

1. Focal points, markers and spoilers.

This Article is about “marker” and “spoiler” offenses against focal points in an objective cyberspace.27 A “marker” is an expression used as an address or magnet to draw traffic in space.28 A “spoiler” is an expression that functions as a roadblock or detour in cyberspace.29 A “focal point” is a belief about behavior that has some kind of psychological salience, often used in game theory to explain some game-optimal solutions, especially equilibrium points.30 Here is a common focal point illustration:

26 Indeed, if some history might be as necessary as truth-claims in the development of new scientific paradigms, the same should be no less true in the development of a law for cyberspace. See THOMAS KUHN, THE STRUCTURE OF SCIENTIFIC REVOLUTIONS 1 (2nd ed. 1972) (observing: “History, if viewed as a repository for more than anecdote or chronology, could produce a decisive transformation in the image of science by which we are now possessed.”)

27 An objective cyberspace is an embodied, coded, switched network for moving information traffic further characterized by varying degrees of access, navigation, information-activity, and trust. It includes the phone system and the Internet, among other things. See infra, Section I.B.2. (discussing cyberspace). This Article eventually defines the more significant terms in the course of discussing them, but a reader who wants to survey the development of the concepts may refer to the prior Articles, supra notes 15-18, and a reader who simply wants to make use of the supporting glossaries and summaries may refer to the Appendices referenced, supra note 24.

28 A descriptive, or vanity domain name (www.Moviebuff.com) or telephone number (1-800-HOLIDAY) are examples of “markers.” These two examples each incorporate trademarks, but markers need not do so (consider, e.g., www.movies.com or www.hotels.com). There are many other possible markers, and my terminology is not dependent upon any specific technological application or any particular happenstance of how they occur.

29 A preemptive registration of another person’s name or trademark in a domain which permits only a single identical registration is an example of a “spoiler.” There are many other ways to spoil or waste navigational markers in space, and my terminology is not dependent on any one method or technique.

Two friends are supposed to meet at noon in Paris, but they forgot to decide on a specific meeting place. Both might well go to the Eiffel Tower at noon, expecting the other to do the same, given that it’s one of the most famous landmarks in the city. In this case, meeting at the Eiffel Tower might be a focal point.\textsuperscript{31}

It is a short leap to understand the power of focal points in cyberspace as an aid to, or potential hindrance of navigation. Someone wanting to call Holiday Inns to find a Holiday Inn hotel, but not knowing the phone number might guess a focal point and so might dial 1-800-HOLIDAY, especially if there has been a promotional campaign making the focal point association.\textsuperscript{32} Someone wanting to find a place on the world wide web featuring one or more of the persons who have used MOVIE BUFF (with a space between the words) or MOVIEBUFF (without a space between) for movie-related products or services might enter the expression “movie buff” or “moviebuff” into a search engine’s search window, or might even try to form an address using one of the terms, as by guessing something like www.MOVIEBUFF.com and entering it into a search engine’s address window.\textsuperscript{33}

Someone wanting to block access to, or divert traffic from a location associated with another person, place or community of interest might register or warehouse key focal points, perhaps finding some opportunity for arbitrage by selling them at a higher price to some representative of those persons, places or communities. Someone who desires to provide targeted advertising keyed on focal points, to sell eyeglasses or contact lenses, for example, might intercept the expression “contacts” as entered by some user and return one or more invitations to the user to click on links to various providers of related goods or services.\textsuperscript{34} The same sort of targeting might be “non-commercial” but still triggered by focal points and still characterized as an invasive intercept followed by invitation.

The particular power of focal points in space derives from the fact they are dynamic. Focal points are dynamic or “live” in cyberspace because they are of more than psychological salience. Unlike the case of the Eiffel Tower in ordinary space, where a person might say “Eiffel Tower” as often as she pleases without going anywhere, uttering a dynamic focal point into a machine in cyberspace can actually change a user’s objective relationships.\textsuperscript{35} Focal points in space can

\textsuperscript{31} Id. at 47. The game assumes incomplete knowledge, and even though rated as game optimal or sub-optimal, the selected focal point provides no guarantee of success—one of the players may have guessed Arc de Triomphe.

\textsuperscript{32} See Holiday Inns, Inc. v. 800 Reservation, Inc., 86 F.3d 619 (6th Cir. 1996) (evidencing such conduct on the part of persons seeking to find Holiday Inns, trapped by a deceptively similar pneumonic phone number).

\textsuperscript{33} See Brookfield Commc’ns, Inc. v. W. Coast Entm’t Corp., 174 F.3d 1036 (9th Cir. 1999) (evidencing two legitimate users of the expression, one having used the expression “movie buff” as part of a composite slogan with a space between the words and subsequently having registered a domain name, “moviebuff.com,” without a space between words, and the other having obtained a federal trademark registration for the expression “moviefull”). In the court’s opinion, it apparently made a difference for purposes of “tacking,” if not for likelihood of confusion under trademark law whether the contested expressions included a [space] between the words “movie” and “buff” or not. This particular domain name is currently offered for sale at a quoted price of $20,000, DomainMarket.com (“click to buy MovieBuff.com for $20,000”) last visited on November 28, 2009 (accessed by entering “www.moviebuff.com”).

\textsuperscript{34} See 1-800 Contacts, Inc. v. WhenU.Com, Inc., 414 F.3d 400 (2d Cir. 2005) (evidencing such conduct on the part of persons providing targeted advertising, triggered by typing a trademarked expression of another).

\textsuperscript{35} Compare THE WIZARD OF OZ (Metro-Goldwyn-Mayer 1939) (Dorothy repeats “there’s no place like home, there’s no place like home…” while clicking a pair of ruby slippers) with the effect of clicking on a live hyperlink on the worldwide web side of cyberspace. One only works in the imagination (from Oz to Kansas, as
actually deliver a person’s augmented presence to a location where the user can see and hear sights and sounds, interact with, and be acted upon by others, all leaving an objective trace.

I claim the deliberate misuse of focal points in cyberspace constitutes a form of actionable misrepresentation or deceit, theft or misappropriation, spoilage or unfair competition. This result follows either (a) under ordinary principles of law as developed in “ordinary space” and more or less directly transposed, mutatis mutandi, to cyberspace, or else (b) under principles of ordinary law deliberately transformed to choose the architecture of cyberspace that best preserves the values characterizing a useful, enjoyable and valuable place in the code world. By either provenance, recognizing this cyberspace offense is a step toward creating a law purposely designed for cyberspace, and deliberately intended to influence the architecture of the code world. These offenses are characterized by an abuse of dynamic focal points in cyberspace.

An offending focal point offense comprises deliberate and calculated deception, misappropriation, waste or unfair competition in an objective cyberspace which relies upon a virtual map characterized by reliable markers, addresses and magnets. The cyberspace focal point offender tampers with or alters the map, plants deceptive markers, ambushes users, or expropriates and spoils markers that point towards other persons, places or communities of interest.

The need to reframe the issues, and even to explain them, has required that there be words to name them. In my prior Articles, I have developed a vocabulary that is “new” only insofar as it provides shorthand ways of naming and then analyzing well-recognized patterns that are routinely occurring in cyberspace and have become part of the ordinary experience of most persons who will be reading this—there is nothing exotic, esoteric or even particularly “novel” about any of these things. They have merely lacked convenient names.

2. Invisible and attenuated likelihood of confusion (when trademark law fails).

These focal point offenses intersect with trademark law. When the offending actor’s marker or spoiler also incorporates a trademark of another person, the actionable cyberspace focal point offense is compounded and may often constitute at least an attenuated form of trademark infringement. But trademark infringement, vel non, is accidental to the essential harm. Deceit or misrepresentation, theft or misappropriation, and waste or unfair competition by abuse of dynamic focal points is already a serious problem in cyberspace regardless whether the actor incorporates someone else’s trademark within its otherwise offending marker or spoiler.

portrayed in a motion picture, as derived from a storybook, and as an imagination or as a shared imagination), the other actually works in an objective place. The objective cyberspace is not an imaginary domain, much less a consensual hallucination.

36 A glossary is reproduced in Appendix B.

37 Though perhaps finally going out of style, it has been asserted that actors who use trademarked expressions of another in cyberspace in a manner that is invisible or attenuated are exonerated from trademark liability altogether because the offending conduct does not involve the “use” of the expression “as” a mark. Even if this were not bad trademark law or policy, see infra text at notes 54-73 (setting forth the argument, and summarizing some of the cases and the commentaries), it obscures the fact that the expression is being used as an abusive focal point which should at the very least raise the question whether there is a much more fundamental
Although the presence of a trademark is not essential to the underlying focal point offense, it would have seemed the presence of a trademark only makes the underlying focal point offense more egregious, harmful, and (one would have thought) easier to discern, label, and proscribe. But instead of making things easier to resolve, the presence of trademarks has had the opposite effect. This is because the code world permits expressions, including trademarks, to be perceived, reproduced and communicated by machines even if not by human consumers. Copyright law has finally rid itself of the anti-technology bias typified by the White-Smith reading of copyrights and “copies.” Not only has trademark law not yet given up its similar bias, it is currently ill-equipped to do so. My new navigational markers and a virtual map to cyberspace, potential benefit, constituting a public good when employed fairly to establish conclude that such expressions constitute dynamic focal points that are of great draw or hinder traffic in space. From a cyberspace perspective, it is not difficult to understand. It is a direct consequence of the dynamic focal points which exist in cyberspace, without any strongly analogous reality or legal precedent in ordinary space. Consider that a dynamic focal point—a marker, a spoiler, an address, magnet, roadblock or detour—may be a machine readable expression. This means a focal point is an expression that might be invisible to a human user, only remotely associated with goods or services offered for sale, not accompanied by any obvious or direct advertisement or promotion, and yet it can very effectively draw or hinder traffic in space. From a cyberspace perspective, it is not difficult to conclude that such expressions constitute dynamic focal points that are of great potential benefit, constituting a public good when employed fairly to establish navigational markers and a virtual map to cyberspace, but causing significant problem going on in cyberspace, and whether the law might be better designed if it were to attempt to solve the underlying problem directly and explicitly rather than by imagining that trademark must be the answer to every question, as if it were some sort of philosopher’s stone.

---

38 White-Smith Music Co. v. Apollo, 209 U.S. 1, 17 (1908) (defining a copy of a musical composition, for purposes of copyright infringement, to be “a written or printed record of it in intelligible notation” and observing that the musical tones produced by the player piano roll at issue in the case were “not a copy which appeals to the eye”).

39 White-Smith by its terms affected copyright infringement by unauthorized copies, but its ramifications also extended to creation and publication of works of authorship in tangible copies. Cf. White-Smith, supra, 209 U.S. at 17 (“A musical composition is an intellectual creation which first exists in the mind of the composer. . . . It is not susceptible of being copied until it has been put in a form which others can see and read.”). Observant commentators have pointed out that “[w]hile the outcome of the case was overruled by the 1909 [Copyright] Act, its way of thinking survived until the 1976 [Copyright] Act was passed—and even beyond.” CRAIG JOYCE, MARSHALL LEAFER, PETER JASZI & TYLER OCHOA, COPYRIGHT LAW 65 (7th ed. 2006).

40 This is an instantiation or transposition of the “hitchhiker’s guide to the galaxy” from a work of fancy (or prediction) to the reality of the constructed cosmos of cyberspace—what had previously been imagined is now made real and it dwells among us (or we with it). Think of a phone without a phonebook, and then think of cyberspace without a virtual map or index. While I carry no brief for Google, Inc., it is a manifest fact that Google has delivered something which might have seemed practically impossible, and which is certainly good for cyberspace access, navigation, information-activity, for those who use it, including the hitchhiker, surfer and ordinary folk, and directed towards a common good suitable for public policy support. The hitchhiker, and the developing laws of the polity, might want more explicitly to consider the benefit to the common good provided by the hitchhiker’s guide before over-regulating space. See, Folsom, Space Pirates, supra note 17 (dividing space pirates from hitchhikers and guides in cyberspace and proposing that a law rationally designed for cyberspace should distinguish guides from pirates, and should incentivize or at least permit the guide while disincentivizing the pirate or predator); compare DOUGLAS ADAMS, THE HITCHHIKER’S GUIDE TO THE GALAXY 3 (Del Rey 1997) (1980) (valuing a guidebook that is at least occasionally accurate and “cheaper than its closest competitor.”)
harm when abused. 41 From a realistic cyberspace perspective the problem is easy to identify and its obvious solution is to encode a reasonable technological accommodation, at least upon request. 42 But from a traditional trademark perspective, the problem is much more difficult to recognize, and the solution much more elusive. 43

The failure of trademark law. I have written more than one prior Article for the purpose of permitting brevity here. Notwithstanding this, some repetition may be in order. My claim is that traditional trademark law has failed, is failing, and will almost certainly continue to fail to handle invisible and attenuated uses (focal point offenses) in an objective cyberspace. A condensed version of the argument is presented here, and a complementary version is appended as Appendix B.

Traditional trademark law is in the position of providing a toolbox that contains only a hammer when the target might not be a nail. 44 Traditional trademark law has been asked to handle what, from a trademark perspective, is a near impossibility. Trademark law has been asked to determine whether, and if so when exactly there can be a likelihood of confusion caused by an invisible or attenuated use of expression to draw or block traffic, 45 notwithstanding the

41 Predatory and piratical conduct can be defined in cyberspace, and the notion that the virtual map can be blithely altered, destroyed, tampered with, spoofed, blocked, wasted or ruined, or that malicious mischief is somehow transformed into protected speech or expression because it happens to be instantiated through the language of constructed code would seem as alien and perverse to any rationally designed law for cyberspaces as it would be in any ordinary space in which the same sort of thing could happen. Imagine that a person could simply speak “poison” in ordinary space and then serenely watch all the neighboring dogs die—(this, of course, describes what we would describe as a form of “magic” or other supranatural effect in ordinary space). If such magical things occurred in ordinary space as a direct effect of language, caused by a person who spoke the words; if the effects of such speech were directly and objectively demonstrable, reproducible, and regular; and if they could be proved or falsified by any reliable forensic evidence, is there any doubt they would be regulated? [see C.S. Lewis on point]. Of course, because those conditions are rather obviously not the fact in ordinary space, it follows that ordinary space is not, and should not be so regulated. But regardless of the state of observable reality in ordinary space, and directly contrary to it, the power of code in the code world trivially includes the routine power to affect real relations and to change the objective state of the code world merely by utterance of coded expression. It follows, and not only because these conditions are a fact in cyberspace, but also constitute a fact that as much as anything distinguishes the code world from ordinary space, such conduct should be regulated in cyberspace and elsewhere in the code world, at least if there is to be any sort of rationally designed law that is developed with the reality of the code world in mind. See Space Pirates, supra note 17 (isolating and defining space pirates and predators, and urging that they be regulated).

42 An example of this sort of technological accommodation is the one reached between Martha and Dank whichmade the poisonous flowers lose their poison when they leave Martha’s property without her consent. In ordinary space, there are all sorts of competing interests and expenses. In the code world, it is sometimes just a simple matter of loss-less recoding. See text at notes 1-6 supra.

43 An example of the same sort of mismatch between ordinary law and the manifest reality of the code world is that which could have arisen in the case of the poisoned flowers; from the perspective of traditional nuisance law, the poisonous flower problem might have seemed insoluble. The tragedy of automatically inflicting ordinary law upon cyberspace is that even though a technological resolution in the code world might be simple, efficient and optimal, there is perhaps no ready-made rule of ordinary law to force it upon a willful offender.

44 If the only tool is a hammer, then the tendency is to think every problem must be a nail. See ABRAHAM MASLOW, PSYCHOLOGY OF SCIENCE 15 (___) (“I suppose it is tempting, if the only tool you have is a hammer, to treat everything as if it were a nail.”) (sourcing provided by http://groups.google.com/group/google-mac-news/browse_thread/thread/ae2f669678aceb3, last visited on 25 Nov 2009). Compare “if I had a hammer [then] I’d hammer in the morning, [and] I’d hammer in the evening all over this land… Well, I’ve got a hammer… [and I suppose] it’s the hammer of justice…” Pete Seeger & Lee Hayes, If I had a Hammer (1949). One would hope the “hammer of justice” might hit some “nail” calculated to secure justice rather than striking some random target, and especially one might hope that any “nail” to be driven and not broken by the hammer might be made out of something other than fine china.

45 I use two expressions almost interchangeably, but based on the perspective. From the perspective of cyberspace, the activity involves dynamic focal points which are markers or spoilers used as addresses, magnets,
obvious difficulties inherent in the mere statement of the problem. A moment’s thought will reveal the difficulty. If a use is “invisible” to a human user or if it is “attenuated” and remote from a directly observable association with competing or substitutionary goods or services, how can it be rationally supposed to cause a “likelihood of confusion” in the minds of an appreciable number of reasonable consumers? And even if an invisible or attenuated use could do so, how would anyone know how to recognize it according to any useful legal test?

It is not at all surprising that one line of trademark cases responded to these riddles by embracing one extreme. This first line of cases over-protects trademarks in space on the seemingly sensible (but ultimately unworkable and factually unsupportable) view that all such attenuated expressions cause an “initial interest”; that such interest must rise to the level of “initial interest confusion” prior to the point of sale; and therefore such initial interest confusion must, even if dispelled prior to sale, necessarily result in an almost automatic finding of actionable “likelihood of confusion” in cyberspace. 46

Subsequent commentators include a few who have endorsed 47 and many who have criticized 48 the so-called Brookfield 49 over-protection approach. Subsequent cases, including one in the jurisdiction in which this line of cases arose, 50 have backed away from this approach, and it seems to be waning. 51 In my prior articles, I have criticized this line of cases for misapplying the doctrine of initial interest roadblocks or detours. From the perspective of traditional trademark law, the best formula is that which describes the problem as assessing likelihood of confusion arising out of invisible or attenuated uses. It should be clear that there are other, more orthodox ways to use trademarks in cyberspace, but the focal point offenses and related trademark offenses involving invisible or attenuated uses comprise those that are the most difficult to resolve under current rules. My primary concern is with those difficult cases.

46 Playboy Enters. v. Netscape Commc’ns Corp., 354 F.3d 1020 (9th Cir. 2004); Brookfield Commc’ns, Inc. v. W. Coast Emm’t Corp., 174 F.3d 1036 (9th Cir. 1999); Missing the Mark, supra note 16, at 181-96 (selecting these two cases as representative and asserting that both Netscape and Brookfield “overprotect” marks in cyberspace compared to ordinary space by creating trademark liability in cyberspace greater than, and in conflict with, ordinary principles of trademark-related law). The overprotection stems from a radical misapplication of the “initial interest confusion” doctrine in cyberspace—the only correct application of that doctrine in cyberspace must require that there be a preclusive-style of initial interest confusion, which is probably rare although not impossible in cyberspace. Id

47 E.g., Chad J. Doellinger, Trademarks, Metatags and Initial Interest Confusion: A Look to the Past to Re-Conceptualize the Future, 41 IDEA 173, 200, 219, 225 (2001) (noting that Brookfield’s application of the initial interest confusion doctrine was too broad, but arguing that “[t]he mere appearance of [the] defendant’s web site on a search engine results list necessarily indicates consumer confusion at a certain level” and the initial interest confusion doctrine, properly understood, is the correct way to apply trademark law to metatag and search engine use of trademarks).

48 See, e.g., Zachary Zweihorn, Searching for Confusion: The Initial Interest Confusion Doctrine and Its Misapplication to Search Engine Sponsored Links, 91 CORNELL L. REV. 1343, 1357, nn.98 & 100 (2006) (pointing out that the billboard analogy used to discuss initial interest confusion on the internet has been “widely criticized” and perhaps more so by younger persons “more attuned to how the Internet works”); Joseph V. Marra, Playboy Enterprises, Inc. v. Netscape Commc’ns Corp.: Making Confusion a Requirement for Online Initial Interest Confusion, 20 BERKELEY TECH. L.J. 209, 213 (2005) (Brookfield’s reliance on initial interest confusion is misplaced); Perry Viscouncty & Jordan Kushner, Order to Confusion: Trademark Infringement Liability for Search Engine Keying Ads, 1 HASTINGS BUS. L.J. 151, 153, 156-57 (2005) (search engines are not “using” trademarks in the traditional sense, and the logical extension of the initial interest confusion doctrine to such conduct would be overprotection).

49 So designated from the case most commonly cited for the doctrine, Brookfield Commc’ns, Inc. v. W. Coast Emm’t Corp., 174 F.3d 1036 (9th Cir. 1999).


51 See Folsom, Defining Cyberspace, supra note 15 at 110-12 and nn. 88-91 (observing the billboard analogy is not only wrong, but exactly backwards).
confusion in cyberspace insofar as it would make nearly “all” initial interest actionable and eligible for the full battery of trademark infringement remedies even though there is no realistic likelihood of confusion in many if not most cases, and even though a much more modest technological remedy would have sufficed to remove any underlying focal point harm.\textsuperscript{52} At the same time, I have pointed out there actually might be some cases in which there really is, or at least might very well be, a true preclusive-style initial interest confusion in cyberspace and in which trademark infringement by likelihood of confusion may well have been present.\textsuperscript{53}

It is equally unsurprising that another line of trademark cases, represented by 800 Contacts and Holiday Inns,\textsuperscript{54} responded by embracing the opposite extreme in cyberspace. These cases under-protect marks in space on the strangely attractive but utterly novel theory (or “defense”) that there is a threshold “use” requirement which must be met prior to assessing likelihood of confusion.\textsuperscript{55} According to this view, if the “use” is invisible, unadvertised, unpromoted, or only remotely associated with goods or services then the offending conduct cannot constitute “use” of the offending expression “as” an actionable offense within the meaning of trademark law.\textsuperscript{56} Because the pertinent statements of the rule for trademark liability in ordinary space all depend upon some offending “use” which causes a likelihood of confusion,\textsuperscript{57} then it could follow that none of the offending invisible or attenuated conduct relating to marks in space can possibly constitute trademark infringement, even if such conduct is not only intended to cause confusion or deceit but actually does.\textsuperscript{58}

\textsuperscript{52} See, e.g., Folsom, \textit{Defining Cyberspace}, supra note 15 at 110-12 and nn. 91 & 92 (suggesting actual preclusive-style initial interest confusion may arise in cases involving trapping addresses and in cases involving the photographs of naked models).

\textsuperscript{53} It is ironic that this approach, though soundly criticized, may actually have occasionally and almost accidentally reached the right result, albeit for the wrong reasons—where there actually was preclusive-style initial interest confusion in cyberspace. \textit{Id.}

\textsuperscript{54} 1-800 Contacts, Inc. v. WhenU.com, Inc., 414 F.3d 400 (2d Cir. 2005); Holiday Inns, Inc. v. 800 Reservation, Inc., 86 F.3d 619 (6th Cir. 1996); Folsom, \textit{Missing the Mark}, supra note 16, at 196-213 (selecting these two cases as representative and asserting that both 1-800 Contacts and Holiday Inns “underprotect” marks in cyberspace compared to ordinary space by refusing, in conflict with ordinary principles of trademark-related law, to find any basis upon which even to apply the law to allegedly offensive or clearly predatory mark-type activity in cyberspace).

\textsuperscript{55} This characterization is, of course, my own, supported, \textit{en passant}, in my prior Articles. The cases themselves certainly do not admit to being a novelty. Indeed, analyzing such cases, Professor Barrett has very ably argued for the proposition that the asserted requirement is, in fact, of ancient provenance in the common law, and she is not alone. \textit{See infra} note 59. Although I disagree with those interpretations, as well argued as they may be, a major, and perhaps core concern of my own has been to avoid the controversy which seems sterile, and rather to propose a new approach which is at once more workable and more tuned to the needs of the code world. It might be fun at some point more directly to enter into the fray, but it seems more important to present a comprehensive resolution which explicitly designs law for cyberspace by taking full advantage of the coded nature of that world and the common good that constitutes a discernable basis for developing public policy there.

\textsuperscript{56} \textit{Id.}

\textsuperscript{57} \textit{See} \textit{AMERICAN LAW INSTITUTE, RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 20 (1995)} (“One is subject to liability for infringement of another’s trademark… [if] in identifying the actor’s business or in marketing the actor’s goods or services the actor uses a designation that causes a likelihood of confusion…”) (emphasis added); Lanham Act § 32, 15 U.S.C. § 1114 (“Any person who shall, without the consent of the registrant… use in commerce any… colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services or on or in connection with which such use is likely to cause confusion… shall be liable in a civil action by the registrant…”) (emphasis added); Lanham Act § 43(a), 15 U.S.C. § 1125(a) (seemle, for unregistered marks).

\textsuperscript{58} \textit{See} Holiday Inns, Inc. v. 800 Reservation, Inc., 86 F.3d 619 (6th Cir. 1996) at ___ (reversing judgment notwithstanding trial court’s findings).
Subsequent commentators include some who have endorsed, some who have criticized, and some who have noted the apparent brief ascendancy of this “use” requirement or defense. But more recent cases, including in one of the jurisdictions in which this line of cases arose, have backed away from this approach, and they may well signal its decline and eventual demise. Some commentators seem to agree that the doctrine is waning while others offer to

---

59 E.g., Margreth Barrett, Finding Trademark Use: The Historical Foundation for Limiting Infringement Liability to Uses “in the Manner of a Mark”, 43 WAKE FOREST L.REV. 893 (2008) (finding an historical common law formulation, and proposing a modern trademark use limitation, requiring that the offending expression be applied in a manner: “(1) that consumers can perceive with their senses; (2) that closely, directly associates the word or symbol with products or services that the defendant is advertising, selling, or distributing to consumers; and (3) that it is likely to make a separate commercial impression on consumers.”); ULI WIDMAIER, USE AND THE STRUCTURE OF TRADEMARK LAW, 33 Hofstra L. Rev. 603, 704 (2004) (applauding Holiday Inn as the better approach to the problem: cases like Holiday Inn have “stubbornly insisted upon proof of trademark use of the allegedly infringing mark by the defendants themselves. That is the correct viewpoint, and the doctrinal nail in the coffin of the Brookfield . . . aberration.”). See generally Graeme B. Dinwoodie & Mark D. Janis, Confusion over Use: Contextualism in Trademark Law, 92 IOWA L. REV. 1597 (2007) (expressing skepticism that there is a separate “use” “as” a mark requirement while noting that there are those who have proposed such a requirement); STACEY L. DOGAN & MARK A. LEMLEY, GROUNDING TRADEMARK LAW THROUGH TRADEMARK USE, 92 IOWA L. REV. 1669 (2007) (relying to Professors Dinwoodie and Janis, and advocating a separate “use” requirement: “[t]he trademark use doctrine has always played a central—albeit implicit—role in trademark law.”).


61 In their popular trademark casebook, and prior to pointing out their own skepticism that there is any such separate use requirement, Professors Graeme Dinwoodie and Mark Janis concede that “the balance of scholarly commentary appears to favor a ‘trademark use’ requirement.” GRAEEME B. DINWOODIE & MARK D. JANIS, TRADEMARKS AND UNFAIR COMPETITION LAW AND POLICY 472 (2d ed. 2007) (collecting commentators who apparently favor such a requirement).

62 Rescuecom Corp. v. Google Inc., 562 F.3d 123, 127-31 (2d Cir. 2009). The court seemed to back away from the implications of its prior opinion in 1-800 Contacts and concluded a careful exercise in statutory construction by reasoning that using a keyword that includes a trademark to generate advertising through internet searches is actionable under the Lanham Act. Id. at 130-31. The court further explained that the question of the likelihood of confusion turns on the particular circumstances surrounding the manner in which the allegedly infringing website is presented to the consumer. Id.; and see N. Am. Med. Corp. v. Axiom Worldwide, Inc., 522 F.3d 1211, 1218-19 (11th Cir. 2008) (distinguishing 1-800 Contacts on the basis that Axiom’s metatag uses resulted in some visual display, id. at 1219-20, and yet going so far as to say: “[T]o the extent the 1-800 Contacts court based its ‘use’ analysis on the fact that the defendant did not display the plaintiff’s trademark, we think the Second Circuit’s analysis is questionable).”

63 Cases continue to percolate and the ultimate resolution remains in doubt, but some of the post-Rescuecom trial court decisions as of the cutoff date of this article and which suggest the decline of the separate “use-as-a-mark” requirement for infringement include: Morningware, Inc. v. Hearthware Home Prods., 2009 U.S. Dist. LEXIS 106615 (N.D. Ill. Nov. 16, 2009) (ruling that a competitor’s purchase of a keyword trigger meets the Lanham Act’s use requirement even though the competitor asserted it had never placed that term on any product, good or service, or used it in any way that would indicate source or origin); Fair Isaac Corp. v. Expertan Info. Solutions, Inc., 2009 U.S. Dist. LEXIS 64022 (D. Minn. July 24, 2009) (holding that “purchasing keywords containing a trademark to generate advertising from internet searches constitutes ‘use in commerce’ as required to maintain a claim of trademark infringement under the Lanham Act; that the question whether defendants’ sponsored advertisements ‘actually include’ the trademarks ‘is not determinative of whether there has been any infringement’ and that likelihood of confusion would turn on the particular facts surrounding the manner in which the allegedly infringing website is presented to the consumer). See also Hampton Locations, Inc. v. Rubens, 640 F. Supp. 2d 208, 221, ___ and n. 11 (E.D.N.Y. 2009) (holding there is no “use” requirement under the Anticybersquatting Consumer Protection Act, and noting that “[Rescuecom] questions whether the definition of ‘use in commerce’ found in §1127 (§45 of the Lanham Act) . . . even applies to alleged infringers under the Lanham Act” because Rescuecom indicates that “the definition of ‘use in commerce’ should only apply to those portions of the Act prescribing eligibility for registration, and not the sections defining infringing conduct.”)

64 See generally, Margreth Barrett, Internet Trademark Suits and the Demise of “Trademark Use”, 39 U.C. Davis L.Rev. 371 (2006) (discerning an expansion in trademark rights in the Internet context: part of the expansion due to the application of the initial interest confusion doctrine and “an equally great cause of the expansion may be the courts’ movement away from the requirement that infringement... defendants make a
mediate the controversy or urge that much or all of what I call “invisible and attenuated” uses simply ought to pass without trademark scrutiny or else be regulated as a matter of misappropriation, properly understood.

In my prior articles, I have criticized the 800 Contacts and Holiday Inns line of cases and the “use” requirement. Not only is the “use” requirement a novel and unwarranted reading of normative trademark law and many of its fairly standard applications. Not only does the “use” requirement exonerate predatory, deceptive, and fraudulent conduct, leaving no common law legal recourse against invisible and attenuated conduct causing likelihood of confusion (and actual confusion or fraud) in cyberspace. Worst of all, it is inelegant because unnecessary and overly-designed.

If the mark-related problems in cyberspace are a subset of focal point problems, and if focal points can be regulated by code to eliminate or mitigate piratical and predatory conduct while still permitting robust access and navigation, then the better solution must be to deal with focal points directly, and with the focal point remedy limited to reasonable technological accommodations. The trademark “use” defense, considered as a means to prevent the over-protection of marks in cyberspace and as a check against the overly expansive “initial interest confusion” line of cases is simply not needed to regulate focal point abuses of markers and spoilers in space. This is so even when the focal points contain trademarked expressions.

Finally, it is not surprising that if, and when, both lines of cases (or the more doctrinaire reading of them) should fall into disrepute, then there is, or will be, a real and much more difficult problem looming for current trademark law when confronting the invisible and attenuated uses that constitute the paradigmatic new uses in cyberspace. That is, if we reject not only the Brookfield rule of thumb which prohibits nearly “all” attenuated uses, but also reject the Holiday Inns-800

[65] Mark P. McKenna, Trademark Use and the Problem of Source, __ U. ILL. L. REV. 773 (2009) (offering to mediate the “use” requirement debate: asserting that while trademark use is a predicate of Lanham Act liability, those who advocate treating trademark use as a threshold question “put much more weight on the concept than it can bear.”).

[66] Eric Goldman, Brand Spillovers, 22 HARV. J.L. & TECH., 381 (2009) (conceiving of “brand spillovers” in ordinary space and in cyberspace as positive externalities which increase the profits of third parties who do not own the mark, and asserting that just as there is common immunity from trademark scrutiny for brand spillovers in ordinary space, so should there be in cyberspace.)

[67] David W. Barnes, Misappropriation of Trademark, 9 N.C.J. LAW & TECH. 171 (2008) (proposing a nuanced misappropriation doctrine for application to initial interest confusion on the Internet); and see Lipton, supra note 9 (suggesting a restitutionary doctrine).


[70] Folsom, Space Pirates, supra note 17 at 865 & n. 149 (equivocal uses of the word “use”).

[71] Folsom, Space Pirates, supra note 17 at 865-67 & n. 161-64 (examples of ordinary cases in which there are routine inquiries into likelihood of confusion, notwithstanding an absence of “use” that rises to the level of advertising or promoting the offending expression).

[72] Folsom, Space Pirates, supra note 17 at n. 162 (examples of the harms that would be exonerated).

[73] See supra text at notes 46 and 68-72 (summarizing my views).

[74] Brookfield Commc’ns, Inc v. W. Coast Entm’t Corp., 174 F.3d 1036 (9th Cir. 1999).
Contacts rule of thumb which permits just about everything and prohibits almost “none” of the allegedly offending activity, then it must be the case that “some” invisible and attenuated uses may cause a likelihood of confusion. Once the gatekeeper rules that would divert cases without any need for real likelihood of confusion analysis fall away, then it comes time to try to assess when and where there might be some likelihood of confusion in cyberspace.

The last problem—actually assessing likelihood of confusion for invisible, attenuated or expropriating uses in cyberspace once it is recognized there is no simple heuristic either to prohibit all or to exonerate every such use, but rather each case must be assessed against some meaningful factors—is even more difficult, from the perspective of current trademark law, than the innovative but unsatisfactory rules of thumb just discussed. This is because current factors for assessing likelihood of confusion are inapt when applied to dynamic focal points.\footnote{\textit{See infra} text at notes 236 to 256 (exploring the difficulties of applying existing factors).}

One thing that is certainly correct about both the under-protection and over-protection cases is that it really is hard to find a rational rule to assess “likelihood of confusion” in respect of uses that are imperceptible to users and unmoored to any directly associated product or services. Consider the \textit{Polaroid}\footnote{\textit{Polaroid Corp. v. Polarad Elec. Corp.}, 287 F.2d 492, 495 (2nd Cir. 1961); \textit{and see generally, Restatement (Third) of Unfair Competition (1995) §§ 21, 23 & 24 (semble)).} factors under the assumption that some, but not all “uses” of an invisible or attenuated mark in cyberspace constitutes trademark infringement. Under this assumption, some of those are legitimate uses of a focal point and others constitute actionable wrongs. The last problem is that the ordinary \textit{Polaroid} factors—strength of the mark; degree of similarity between the expressions; proximity of products; likelihood the proprietor will bridge the gap; actual confusion; intent (reciprocal of defendant’s bad faith); quality of the defendant’s product; sophistication of the buyers—may work well enough in ordinary space (or anywhere else that a juridical agent already knows by common experience and practice the “right” answer apart from applying any factors) and yet they don’t work in cyberspace.\footnote{\textit{Id}.}

In cyberspace these traditional factors provide false positives, fail to filter or distinguish, and are often irrelevant, unhelpful and unreliable, leading to non-cogent inferences on the ultimate question of likelihood of confusion caused by invisible or attenuated uses.\footnote{\textit{But see, e.g., Stacey L. Dogan \& Mark A. Lemley, Trademarks and Consumer Search Costs on the Internet, 41 Hous. L. Rev. 777, 838 (2004) (arguing that the law does not need to change to deal with Internet keywords, but courts need to apply existing law correctly); David M. Fritch, Searching for Initial Interest Confusion and Trademark Protection in Cyberspace, 6 U. Pitt. J. Tech. L. \& Pol’y 1 (2005); Daniel C. Glazer \& Dev R. Dhamija, Revisiting Initial Interest Confusion on the Internet, 95 Trademark Rep. 952, 953 (2005); David M. Klein \& Daniel C. Glazer, Reconsidering Initial Interest Confusion on the Internet, 93 Trademark Rep. 1035, 1064 (2003) (arguing that the traditional trademark likelihood of confusion factors, excluding initial interest confusion, together with the FTDA and ACPA are adequate to protect senior users).} Unless we are prepared so radically to redefine the existing factors as to make them unrecognizable in ordinary space, it is almost certainly no good to say simply that we must “more carefully apply” the existing factors, or that some modest additions to, or fine-tuning of the factors might do the trick.\footnote{\textit{But see Eric Goldman, Deregulating Relevancy in Internet Trademark Law, 54 Emory L.J. 507, 584-}} The factors just don’t work very well because they are ill-adapted to
uses that are invisible to consumers and are often unmoored from any direct link to competing goods or services, but which nonetheless alter the virtual map, deceive or ambush users, and spoil cyberspace access and navigation. It certainly seems that no amount of careful, or better, application of current trademark law, untransformed for cyberspace, will solve the problem. Doing the wrong thing better (as by trying more carefully to jury-rig existing likelihood of confusion factors to resolve invisible and attenuated uses in cyberspace) is still wrong.

Rather than disrupting ordinary law for the “odd” cases of cyberspace, it would be better far simply to add a new factor for cyberspace. My proposal does just that: instead of glossing the old, it adds a new factor, applying it only when the “place” of use is cyberspace. The new factor, of course, permits some borrowing and revision of the old factors, but it adds factors explicitly designed for the coded reality of cyberspace and puts a “firewall” between the new relations and corresponding new rules in cyberspace, and the traditional relations and rules developed in ordinary space. It thereby solves the new problem. At the same time, it saves the traditional factors, and preserves the current balance in ordinary space without further complicating life in ordinary space.

It is for this reason that I have avoided, insofar as possible, remaining transfixed within the twin distractions of the “initial interest confusion” controversy and the “use as” controversy in cyberspace. These are both ephemeral, and though very ingeniously devised and thoughtfully advanced, ultimately unpersuasive and unworkable approaches that do not optimally cohere either with traditional trademark law or with the reality of cyberspace. That entire controversy is, to use a currently faddish expression, entirely “orthogonal” to my purpose.83

---

81 This has been implicit in all of the work that has gone before. It would seem that, if likelihood of confusion could be readily discerned in cyberspace, there would have been no need for the rule of thumb that found infringement upon a showing of initial interest, and no need for the countervailing rule of thumb that exonerates invisible and attenuated uses. It has been implicit in my own work, else there would have been no need to design a new “nature and place of use” factor for assessing likelihood of confusion. I have filled the gap, if there be one, by an explicit critique of the existing factor tests, included as Appendix __ hereto.

82 See, Obituary of Dr. Russell Ackoff, WALL ST. J., Nov. 13, 2009 (quoting the management theorist: “All of our problems arise out of doing the wrong things ‘righter.’ The more efficient you are at the doing the wrong thing, the ‘wronger’ you become. It is much better to do the right thing ‘wronger’ than the wrong thing ‘righter’! If you do the right thing wrong and correct it, you get better.”). This quote can also be found at http://naturalfoodsmerchandiser.com/blogs/tabid/84/EntryId/165/The-Right-Thing-Wrong-or-The-Wrong-Thing-Right.aspx.

83 “Orthogonal” in this context has finally made its way to the Supreme Court, and quite possibly might enter into the reports, as the following colloquy attests:

[PROFESSOR] FRIEDMAN: I think—I think that there probably has to be a witness who has observed the procedures … [but] I think that issue [in the question just posed by Justice Kennedy] is entirely orthogonal to the issue here because the Commonwealth is acknowledging —


CHIEF JUSTICE ROBERTS: Oh.

JUSTICE SCALIA: What was that adjective? I liked that.

MR. FRIEDMAN: Orthogonal.

CHIEF JUSTICE ROBERTS: Orthogonal.

MR. FRIEDMAN: Right, right.
Instead, I previously proposed and specified a robust new factor, “the nature and place of use,” for resolving trademark infringement by invisible and attenuated uses of expressions in cyberspace that incorporate trademarks.\(^{84}\)

Fixing trademark law’s likelihood of confusion factors is only part of the solution, however, and the complete solution explicitly reframes the problem away from the trademark perspective. The more comprehensive solution first acknowledges that the fundamental issue involves focal point offenses, and then concentrates upon rewriting the code to resolve focal point conflicts, including those that incorporate trademarks.

3. The Solution (resolving the focal point problem by rewriting the code).

The answer to the question whether the law can touch unexpected and machine-readable new technological uses of focal points which incorporate trademarks in cyberspace should parallel the answer previously formulated to permit the law to deal with machine-recognizable but otherwise unreadable new uses in copyright. The answer should be “yes” and we should learn from the experience of copyright, rejecting in trademark analysis any nascent White-Smith bias.\(^{85}\) That bias, if incorporated into trademark law, would limit or deny the law’s power to deal with technologically enabled trademark-related focal point offenses in cyberspace.

Here is a definition of “use” that recognizes new technologies in trademark law, avoids ducking the issue, and is appropriate for trademark law in the code world:

Any new technological use of a trademarked expression in a manner that may be perceived, reproduced or communicated, directly or indirectly by way of a machine or other device, now known or hereafter developed is not only subject to the focal point analysis but is also a “use” within the domain of potentially offensive conduct which might cause a likelihood of confusion of source, sponsorship or affiliation if in connection with marketing goods or services in commerce. A new technological use includes any conduct by an

\(^{84}\) Folsom, Space Pirates supra note 17. The new “nature and place of use” factor is repeated in this Article in the text at notes 149-159 infra.

\(^{85}\) White-Smith Music Co. v. Apollo, 209 U.S. 1, 17 (1908), see text at notes 38 & 39 supra (discussing what I refer to as the White-Smith anti-technology bias in copyright law).
actor in connection with any coded expression in cyberspace and does not require any advertising, promotion or association that is visible to any human, nor does it require any conduct that would have sufficed to create trademark rights in the actor.\textsuperscript{86}

Limitations against overprotection of marks in cyberspace are no longer to be found in the definition of “use” but are built into (a) the new likelihood of confusion factors, and (b) the limited common remedy which is not only part of the new focal point offense, but is also incorporated into the correspondingly transformed likelihood of confusion factors. There is no need for artificial and anti-technologically biased barriers at the threshold “use” level prior to beginning the trademark infringement analysis.\textsuperscript{87}

One feature of cyberspace is that it is defined and regulated by its architecture. Cyberspace is code, and code can be redesigned and rewritten. As code creates focal point disputes in cyberspace because it enables dynamic addresses and magnets and because it permits operative roadblocks and detours, so a purposefully regulated and redesigned code can be made to resolve those disputes. A purposefully designed law can provide a legitimate lever to require certain actors to recode their offending use of focal points, including those making an invisible, attenuated or expropriating use of someone else’s trademark within an offending focal point.

It is very interesting that Professor Lessig’s example of the poisoned flowers concludes peaceably.\textsuperscript{88} But what if it didn’t? What if the offending actor had refused the simple accommodation of recoding? I propose a very gentle and proportionate, yet unmistakably firm legal push to create just the incentive necessary to induce reasonable recoding in response to focal point offenses: nothing less and nothing more. In so doing, I attempt to make Professor Lessig’s parable a reality, not only without sacrificing any foundational values of cyberspace, but upholding them.

The proposed solution actually makes good on Professor Lessig’s observation that optimal solutions can be deliberately chosen in cyberspace. The focal point offense provides a specified and easily applied baseline (almost a “base case”)\textsuperscript{89}

\textsuperscript{86} The first sentence is modeled in part on the copyright solution: “Copyright subsists in... original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device...” Copyright Act of 1976, §102(a); 17 U.S.C. §102(a). The second sentence clarifies that “use” signifies “conduct” but does not require the level of conduct that could have appropriated trademark rights in the offending expression by “use” of it as a mark.

\textsuperscript{87} See infra (discussing these issues at length).

\textsuperscript{88} LESSIG, supra note 1 at 12-13.

\textsuperscript{89} The parallels between “law language” and code might be worth exploring. See, Folsom, Defining Cyberspace supra note 15 at nn. 3 & 4 (looping footnotes). I use “base case” here not only to signify a legal “case” but with the additional connotations drawn from recursive programming techniques. In a direct sense, and in the code world it is a commonplace that:

If the [recursive] function simply called itself it would never terminate. To end the recursion every recursive function has to have at least one base case. A Base (or Stopper) Case [must be one that] is simple to calculate or has a known solution. It does not require any further recursive calls, and therefore stops the recursion. The base case helps build the solution for the whole problem. Each recursive call must simplify the problem, leading one step closer to the base case(s).

E.g., http://www.c-point.com/javascript_tutorial/recursion.htm (last visited on Dec. 18, 2009). My proposed focal point offense may be considered something analogous to a base case for mark-type offenses in cyberspace,
rule to dispose of most cases, and the complementary “nature and place of use” analysis permits a rational determination whether any trademark infringement has also occurred in the residual set for which greater attention may be justified. The proposed remedy for a cyberspace focal point offense includes one or more responses selected from a set of flexible, proportionate and limited remedies designed to remove just the harm created by the offending code simply by rewriting the code. The remedies include technologically effective disclaimers, notices, forced releases/redirects, reassignments (reciprocal auctions), or opt-outs/opt-ins. The limited remedy cures the harm, upon request and without destroying cyberspace or defacing the law itself.

The new factor has three additional characteristics making it well worth adoption by common law courts and by practicing lawyers. It works. It is economically efficient. It is consistent with recognizable principles of existing law—it is authorized, principled, practical and predictable. The goal of this Article is to persuade judicial actors to apply the proposed solution, *ex ante* in transactional planning, *ex post* in conflict resolution or litigation, and all times in between—to use it in deciding actual cases, and in conducting real negotiations, project planning, development and distribution of new technologies in business. What follows is a step-wise development of the new approach in rule-specific form, moving from what (the focal point offense), to where (cyberspace), by whom (characteristic users), and with what legal consequences (the common remedy), and finally leading to integration (unifying the focal point analysis with likelihood of confusion and other existing mark-related standards).

**B. The Specified Offense**

In this section I develop the new approach in five related steps. These define the offense, the place where it occurs, the people affected, and the limited remedy provided. The last step unifies the field of mark-related problems in cyberspace. Attachment B to this Article extracts these rules from the accompanying text and presents them for reference and review.

1. **The First Step: The Nature of Use (The focal point offense)**

   There are focal points,\(^90\) dynamic focal points,\(^91\) and dynamic focal points breaking out of the loop of trademark law’s current futility. It is also said of recursion, with some parallel to the initially puzzling idea of actionable misconduct arising out of invisible and attenuated uses of marks in cyberspace, that:

   When we experience recursion for the first time, we are usually puzzled. An example of recursion is a magazine cover showing a TV screen showing a magazine cover. The image within an image would be repeated few times before becoming too small to see. Another example is walking between two mirrors. The mirrors are causing mutual recursion. The reflection in the mirror is repeated several times, each one smaller than the previous, before becoming too small to see.

   *Id*. The concept of legal liability for invisible and attenuated likelihood of confusion is initially confounding. The concept of a focal point offense makes it easier to see and to understand. The direct analogy to recursive code, of course, breaks down. The base case is often the last or limiting state in a recursive call, but I propose the focal point offense as the starting condition for legal analysis because it will divert a substantial plurality of cases without having to go through any likelihood of confusion analysis.

   \(^90\) A focal point has psychological salience. See *supra* text at note 30.

   \(^91\) A dynamic focal point is an address, magnet, marker, roadblock or detour in cyberspace or elsewhere in the code world that not only has psychological salience but can deliver an augmented presence to a location, can influence or attract traffic to a location, or can hinder or obstruct navigation.
which incorporate someone else’s trademark. We are already familiar with focal points in ordinary space, as by using “the Eiffel tower” as a game optimal solution. The special features of cyberspace create the new phenomena of dynamic focal points. A dynamic focal point has the power, when uttered into a browser or other machine or device, to deliver an augmented presence to a location. Dynamic focal points can be inherent or associative. Among those which are associative, perhaps the most powerful are those which incorporate the trademark of another person. Existing trademark law is ill-equipped to handle the problem of dynamic focal points which incorporate trademarks.

Here is a one sentence, rule-specific definition of the independently actionable focal point offense:

In an objective cyberspace which relies upon a virtual map featuring dynamically coded focal points functioning as markers and spoilers (addresses, magnets, roadblocks or detours), any conduct which

(a) alters the map (“tampers”),
(b) plants deceptive focal points (“spoofs”),
(c) ensnares a user of focal points with uninvited or false invitations

See supra text at note 31.

In the context of note 31, supra, “the Eiffel tower” is an inherent focal point.

By “associative” I signify a focal point that one of the players has, in a sense, created and which the other player knows about and thereafter associates with him or her. Likewise, if one of the players knows something about the other player, there might be a focal point associated with the other which can lead to a higher certainty solution. This is, perhaps, a loose usage of the game-theory expression, but one that is meaningful in the context of focal points that incorporate trademarks.

Given the definition of a trademark as any “word, name, symbol, device, or other designation, or combination of such designations, that is distinctive of a person’s goods or services and that is used in a manner that identifies those goods or services and distinguishes them from the goods or services of others,” AMERICAN LAW INSTITUTE, RESTATEMENT (THIRD) UNFAIR COMPETITION § 9 (1995), it follows that every trademark is an associative focal point (though not every associative focal point is a trademark).

Trademark law tends to over-protect dynamic focal points which incorporate marks when it imputes a conclusory “initial interest” sort of confusion to any such focal point. Trademark law under-protects dynamic focal points in cyberspace when it supposes the unadvertised or surreptitious placing of a deceptive focal point in connection with marketing goods or services cannot constitute any “use” of an expression “as” a mark even if the conduct causes a likelihood of confusion. Trademark law tends to get the likelihood of confusion factor analysis wrong in respect of dynamic focal points when it seeks to apply standard factors that might be relevant in ordinary space but which create either no inference or else false inferences of confusion in cyberspace. See section __, supra.

An actor alters the map by switching the significance of focal points, so that an inherent focal point no longer has its inherent connection, an associative focal point no longer maintains its associated connection, and an associative focal point incorporating a trademark no longer connects to the trademark-related goods or services.

An actor plants deceptive focal points by initially placing addresses, magnets or markers intended to intercept traffic bound for other persons. “Spoofing” occurs when, for example, an actor learns the artificial intelligence or algorithmic system by which a search engine associates user queries with addressable locations and associated relevancy rankings, and then mimics the characteristics of an addressable location to intercept or divert traffic including by pretending to match or exceed the relevance indicia of the mimiced location. Among the victims of spoofing are the search engines themselves and the resource providers who attempt to make a business based upon providing efficient and reliable searches in cyberspace.
(“ambushes”),\textsuperscript{100} or, “spoils”),\textsuperscript{101} constitutes a focal point offense, subject to the limited common remedy.

It should be understood I am proposing no individual private ownership of, nor “property” in any focal point, but liability-style rules tied to specific offenses. These offenses sound in misrepresentation and deceit, misappropriation and theft, waste and spoilage, all as examples of a particularized and specified development of common law, unfair competition, passing off, and trademark antecedents deliberately adapted to the felt needs of an objective cyberspace.\textsuperscript{102} The limited remedy is integral to the offense and is essential to understanding that the focal point offense is modest.\textsuperscript{103} Moreover, its restricted applicability to an objective cyberspace is essential to understanding that the focal point offense is confined to the code world which spawned the focal point problem in the first place, and is not intended unintentionally to migrate or accidentally to “evolve” into a rule for ordinary space.\textsuperscript{104} It is provided as and to the extent necessary, after request, and it will not encumber cyberspace with extraneous and clumsy regulation.

2. The Second Step: The Place of Use (an objective cyberspace)

Focal point offenses occur in an objective cyberspace. For rule-specific purposes, “cyberspace,” may be defined as an embodied, coded, switched network for moving information traffic, further characterized by varying degrees of access, navigation, information-activity, augmented presences and trust.\textsuperscript{105} Cyberspace includes the Internet,\textsuperscript{106} the phone system,\textsuperscript{107} probably wi-fi,\textsuperscript{108} and much of digital radio and television.\textsuperscript{109} It is aptly observed that what is commonly

\textsuperscript{100} An actor ambushes a user by catching a user off-guard, by intercepting the user’s communications, by invading the user’s privacy or otherwise by trapping, misdirecting or misleading augmented presences, providing unasked-for information, or deluging a user with chaff thereby frustrating navigation.

\textsuperscript{101} An actor spoils focal point by taking focal points out of circulation, by expropriating associative focal points that are associated with another person, or by otherwise wasting focal points. An actor who “warehouses” focal points, has wasted the asset and has spoiled efficient navigation in cyberspace. This applies especially in a cyberspace domain in which it is possible to register and thereby to exclude others from using the registered focal point.

\textsuperscript{102} The characteristics of an objective cyberspace are discussed at step two, section I.B.2, infra.

\textsuperscript{103} The limited remedy is discussed at step four, section I.B.4, infra. It is not only “limited” but is also “common” in the sense that I propose it to be commonly applied to focal point offenses whether arising under current trademark law, anti-cybersquatting statutes, dilution statutes, uniform dispute resolution procedures, or any other regime regulating mark-related conflicts in cyberspace.

\textsuperscript{104} Among other attributes, the code world is modular and self-contained. There is no necessary reason why any law adapted “for” the code world has to be applied to the ordinary world. The code world invites treatment of its problems as if in a laboratory apart from the effect of doctrinal creep back into the ordinary law. See section I.B.2, infra.

\textsuperscript{105} There are many perspectives from which to consider “cyberspace” but this perspective is productive for the purpose of finding a public good which the law might seek to support and from which to develop sensible rules, and without which the discussion is limited to the sterile observation that technology hasn’t any purpose or “essence” much less any moral nature. Folsom, Defining Cyberspace, supra note 15 at 85-87.

\textsuperscript{106} Id. at 87-92.

\textsuperscript{107} Id. at 84.

\textsuperscript{108} Id.

\textsuperscript{109} Id.

\textsuperscript{110} Id. at 85.

\textsuperscript{111} Folsom, Non-Neutral Principles, supra note 18 at 45 & n.3.
called “cyberspace” is really a number of different places. 111 There are observable and different characteristics in each functionally distinct place. 112 Yet these different places within the code world, including cyberspace, all have one thing in common despite their individual differentia. 113 All of them, together with coded places not yet named or developed, are part of an embodied switched and coded network for moving information traffic (the “code world”). The code world is enabled, accessed and navigated by way of machines or devices (the “new machines”) which permit and encourage new technological uses (NTUs) in the code world.

According to my usage, the broadest and most expansive domain is the code world. The code world contains within it “cyberspace” (or “cyberspace proper”), a more narrow place within the code world characterized by varying degrees of (1) access, (2) navigation, (3) information-activity, (4) augmentation, and (5) trust. 114 These five characteristics of cyberspace constitute a straight-forward catalog of reasons why persons value the place. 115 They provide a rational basis for predicating (positing) a public policy, or common good, in cyberspace. Laws or policies which promote robust access, reliable navigation, retrievable and active information, protect augmented presences from the special vulnerabilities faced in

111 See LESSIG, supra note 1 at 82–83 (describing a number of “cyberplaces” each providing a different experience).

112 Folsom, Non-Neutral Principles, supra note 18 at 45 & n.3. In prior Articles, I have referred to the coded domain as the “code world” and to various places within it, including: (1) the “metaverse” as that place within the code world characterized by the consensual association of like-minded persons (communities of interest); (2) “virtual worlds” as those places within the metaverse’s communities of interests, further characterized by a special purpose to participate, almost as citizens in what is almost a polity subject to what is almost a social compact or game; (3) “cypherspace” (or cipherspace) as that place within the code world characterized by a need for trusted, secure and strong encryption, signature authentication, and verified message content for funds transfers, private, secure or secret communications and like activities; (4) the “blogosphere” as that place including the new “press” (where the press is not limited to a newspaper or other traditional distribution channel or medium, but is recognized as any recorded or encrypted means of carrying political speech or current history), (5) “psiberspace” (or psycyberspace) as the human/machine frontier, and (6) “cyberspace proper” as that place within the code world further characterized by access, navigation, information-activity, augmented presences and trust. Id. The code world is the genus, the other places are among the species.

113 All of these places are unified by the fact that they are created by code, and yet are differentiated by the fact that each of them has its own reason for being, and its own specific set of interests, values and regulatory problems. To give them a unifying, generic name, I refer to all of them as being part of the “code world.” When necessary to distinguish particular problems and concerns, I refer to particular parts by name. The particular problems of markers and spoilers most dramatically affect cyberspace proper, hence this Article is most concerned with cyberspace.

114 The five characteristics may be objectively determined, and each admits of varying degrees. Access signifies that the space is “jackable” and that anyone with the right machine can plug in, thereby becoming an addressable user who can both find and be found. Navigation signifies the ability to go from one address or location to other (and, ideally, to all other) addresses, and back again. Information-activity signifies that information, in the widest sense, is a driving object of the space, and that “active” or interactive use of the information is typical. While all new technology “augments” the abilities of its users, the augmentation characteristic of cyberspace is special—the augmented presence of the user is actually extended so that the telephone conversation involves real speech, but at a distance so that while the person remains stationary at a fixed location, the person’s voice is perceived, reproduced or otherwise communicated as an augmented presence at another location, and so with augmented presences on the Internet—these are not “consensual hallucinations” but objective presences. Trust, including trustworthy validation of access, navigational pointers and addresses, information authenticity and content, is necessary if any of these goods are to be maintained. Because augmented presences are especially vulnerable to tampering, trust is all the more important. See Folsom, Defining Cyberspace, supra note 15.

115 They also tend to describe (perhaps only with the benefit of hindsight or induction) what the place was designed to do, or what it has become. From that perspective these characteristics might almost be considered to constitute the design specifications of cyberspace, and to provide a statement of its purpose, end, goal, or function.
space, and foster at least the minimal level of trust necessary to the use and enjoyment of space are “good” for cyberspace.\textsuperscript{116} The contraries are, other things being equal, “bad.”\textsuperscript{117} As a normative and policy matter the law ought to be designed to promote the good and to discourage what is bad for cyberspace.\textsuperscript{118}

Cyberspace proper is important because it embraces the internet, the phone system, wi-fi, and much of modern digital radio and television.\textsuperscript{119} These are among the most useful, enjoyable and commercially valuable applications within the code world. But not all transactions within the code world are equally in need of legal regulation by specially designed rules. Indeed, many and perhaps most transactions in the code world are merely transposed from ordinary space to cyberspace. Just as there may be no need of any special “law of the horse” in ordinary space,\textsuperscript{120} so, in many cases, there may be no need of any special law of cyberspace. But what is needed is a law that is good for cyberspace because it might recognize the new relationships enabled by it, might recognize the public interest in it, and especially because it might recognize that the objective reality of the code world can be changed simply by rewriting the code.\textsuperscript{121}

The advantage of explicitly recognizing a “place of use” factor within cyberspace is that it permits fact-finding on the basic issue: is the conduct even “in” cyberspace at all?—while also recognizing varying degrees of cyberspace. In “low” or “shallow” cyberspace there may be much less need of a special law for cyberspace.\textsuperscript{122} Additional advantages of explicitly defining cyberspace as a potentially significant place are threefold. First, New machines and NTUs in the code world are something like the law’s canary and might provide an early warning to the existence of problems otherwise latent in the law.\textsuperscript{123} Second, NTUs in the code world constitute a modular, coded domain that can actually be broken down and redesigned by simply rewriting the code, if only the law can provide some modest leverage to encourage a redesigned architecture.\textsuperscript{124} Third, and finally,
new machines and NTUs in the code world are important because the possibility of spectacular juridical error is non-trivial and perhaps highly likely. ¹²⁵

Tampering, Spoofing, Ambushing, and Spoiling the Map in Cyberspace. The maps to cyberspace are unique, valuable, and vulnerable. They are especially vulnerable to tampering, spoofing, ambushing and spoiling. For tampering, think of a physical roadway in ordinary space and suppose someone were to alter a warning sign. ¹²⁶ For spoofing, imagine a calculated misrepresentation of the identity, location or nature of a landmark. ¹²⁷ For ambushing, suppose it were possible for someone to listen in to your cell phone conversation and then subsequently to start whispering in your ear, or to insert messages into your GPS system (if you were driving at the time), or to start bombarding your TV with scrolling advertisements (if you were watching at the time). ¹²⁸ For spoiling, think of a medium in which only the first person to register a word could effectively use it. ¹²⁹ The point of listing these actions here is not to assert that each and every instance of technology is deserving of new legal rules “of” the technology involved, but only that we need some legal rule suitable “for” the real persons who are affected, regardless of the specific technology. An additional reason is to focus the discussion on the general nature of the offense by paying attention to what is actually happening in cyberspace because of the power of code to change the state of the coded construct.

The mark-related problem in cyberspace is inherent in the power of dynamic focal points. Focal points can draw traffic, as a magnet. They can deliver an augmented presence, as an address. They can attract a spider to increase a place’s ranking in a search engine index, as a marker. They can also hinder traffic. A spoiler can prevent someone else from using otherwise salient focal points, as a roadblock; can delay or hinder a user in arriving at an intended destination, as a time-wasting detour; or can effectively expropriate an associative focal point, preventing its effective use by anyone. Dynamic focal points can do all these things in cyberspace. ¹³⁰ Offending users have done all of these things in cyberspace. ¹³¹ The law has been ineffective in responding. ¹³² The focal point

¹²⁵ _Id._ at 48 & n. 9 (discussing the conditions for systemic juridical error in cyberspace as an application of the juridical agency problem addressed by Professor Bainbridge and others in differing contexts).

¹²⁶ Instead of “slow down, bridge out” someone might change the sign to read “speed up.”

¹²⁷ Rather than “Louisville, Kentucky” a person might feature “Louisville, Colorado” and so draw traffic several hundred miles out of its way.

¹²⁸ Using blue tooth technology, and phone intercepts this might not be a very remote event, and is just the beginning. Possible psiberspace invasions might tamper with implanted devices, nanotech agents, and augmented medications, not to mention the “ordinary” heart pacemaker. An already-transformed law suitable for dealing with cyberspace offenses may be a good model for designing comparable law to handle the coming psiberspace offenses. _See generally_ note 112 _supra_ (providing a taxonomy of different places within the code world, including psiberspace).

¹³⁰ This is simply to restate the dynamic power of code in a coded world.

¹³¹ These are commonplace occurrences, within the experience of almost everyone reading this Article. _See generally_ Folsom, _Missing the Mark, supra_ note 16 _passim_ (recounting examples from adjudicated cases).

¹³² _Id._ _passim._
analysis I am proposing recognizes dynamic focal points can create problems in
the code world, and it provides a rule-specific form to resolve those problems by
rewriting the code.

3. The Third Step: The Nature of the Users (surfers and mappers, spoofers and
trappers)

Among those persons who characteristically place addresses, magnets, markers
or spoilers in space, or who induce, contribute to or are affected by such conduct
are a characteristic set of users. By nature, these users may be (a) invited or
uninvited, (b) value adding or free riding, (c) helpful, harmless or predatory.

These characteristic users can be further identified to include: (1) surfers and
mappers (hitchhikers and guides), (2) spoofers and trappers (jokers, pirates,
plagiarists and predators), (3) spoilers and arbitrageurs (vandals and economic
rent-seekers), (4) shills and advertisers, (5) shoppers, searchers, consumers,
competitors and mark proprietors.

Some of these are pirates or plagiarists. Again, some of these are targeted
defendants, in the sense they are targeted for secondary liability. Others are
opportunistic plaintiffs, in the sense they are attempting to shift the cost of policing
their intellectual property to targeted defendants. Finally, others are expected yet
often unrepresented “victims,” including the vast numbers of persons who simply
want to use cyberspace and whose interests are rarely consulted in current cases.
The ordinary user, in the capacity of hitchhiker, has an interest in nominative uses
of dynamic focal points simply for cyberspace access and navigation, and that
interest has too often been excluded from consideration. Likewise, the hitchhiker
has an interest in having a reliable hitchhiker’s guide as a resource, and that
interest has been omitted from discussion. Finally, if there is to be a hitchhikers’
guide, and if there is some cost associated with it, perhaps someone should be able
to prepare it without undue concern about potential secondary liability for using
dynamic focal points as navigational (nominative) markers and magnets or as
triggers for high-value contextual advertising sold to help pay for the hitchhiker’s
guidebook.

Cyberspace features and fosters the ability of persons to act simultaneously or
sequentially in more than one capacity. A typical user may shift from one capacity
to another in a single session. Moreover, any given user might in some
circumstances be contextually aware or sophisticated, but might in other
circumstances be situationally or contextually unaware, unsophisticated, and
vulnerable to ambush. As a result of these shifting, fragmented and factional
interests, there is no singular “consumer” interest in cyberspace to serve as the

---

133 Both “pirate” and “plagiarist” have checkered careers in legal discourse, and in my own writing. In this
article, I use the terms in contrast to a person who primarily offends against a clearly marked legal rule (a simple
lawbreaker, or in the context of intellectual property, an “infringer”), and to distinguish these lawbreakers from a
person who primarily offends against a moral intuition or against a social norm of a relevant community to which
the offender belongs (plagiarist) or against a well-demarcated but unwritten or extraterritorial rule of law or who
waste, spoil, and vandalize (pirate). That is, both pirate and plagiarist are always within the genus of deliberate
malefactors; and a plagiarist is always one who “takes” some morally-defined, or some socially-defined (or norm-
defined) credit-worthy language, inspiration, or idea without giving credit. Some (or most) pirates often violate
written or territorial legal rules, and some plagiarists sometimes violate some law (often the law of copyright), but
my usage is intended to give relevant and non-synonymous meanings to the terms.
benchmark “ordinary consumer” for trademark law’s likelihood of confusion test as it has developed in ordinary space.

The nature of the use of focal points in cyberspace is not an arcane or mysterious thing. Surfers, consumers and customers often use focal points to find things: about which they are curious (a user as a surfer), or by use of which they are searching and comparing alternative goods or services (a user as a searcher), or that they want to buy (a user as a customer or shopper). Mappers use focal points to create maps, directories, search engines or other devices to serve as a hitchhiker’s guide to cyberspace. Advertisers, mark proprietors, sellers and their competitors, and anyone else wanting to be found in space use focal points as magnets to attract surfers, consumers, customers and mappers so they, the persons wanting to be found, might be more readily found, considered, and acted upon by the greatest number of those searching in cyberspace. Spoofers, trappers, spoilers, shills and arbitrageurs seek to fool, capture, waste, intrude upon, or take economic rents from those focal points they calculate others (surfers, searchers, customers and mappers) are most likely to consider necessary or useful. Far from being exotic, esoteric or even complicated, the “nature” of use is rather evident, and the evidence depends in no small part upon who is involved, and what they are actually doing.

While the previously considered “place of use” considers where the activity occurs, the “nature of use” explicitly considers who is using, placing, displacing, removing or wasting a focal point, what exactly is being done with or to the focal point, and to whom they are doing it. It also adds an explicit consideration of the public interest and of the generalized interest of persons who are not otherwise before the court. The action itself, determined by the manifest effect of the actor’s use of the focal point, coupled with the actor’s embrace or rebuff of any request voluntarily to rewrite the offending code demonstrates as much or more than any words, and better any other direct or circumstantial evidence whether the use is harmful, harmless and neutral, or beneficial.

The combined “nature and place of use” factor constitutes a rule of thumb distinguishing pirates from guides so the law might disarm the one while encouraging the other. When the actors are evaluated according to their conduct, then labels become both meaningful and helpful in resolving disputes. When the “nature” of the use is conduct offensive to an inherent focal point or to an associative focal point, and the “place” of use is an objective cyberspace where

---

134 Supra, section I.B.2 (the place of use: an objective cyberspace).
135 Reconsider Professor Lessig’s hypothetical poisoned flowers. Assuming a transaction cost-free, Pareto-optimal response to the request to stop poisoning the dog, one would be hard-pressed to avoid the inference that the only person who would refuse such a request is a person who delights in killing dogs. I refer to requests of this sort as “sampling” (or “polling”) and I count the response to such requests as self-proving; as evidence which itself tends to establish a legally operative fact. See infra section I.B.5 and text at note 163. Sampling or polling is inherent in the focal point offense, and is specified as an explicit factor in the new likelihood of confusion analysis.
136 This is in the spirit of the common aphorism “Factum non verbum” (variously rendered into English, including as “actions, not words”). Cf., e.g., Tsinghua [Qing Hua], University (describing itself as being dedicated to the well-being of Chinese society and to world development according to its “motto of ‘Self-Discipline and Social Commitment’ and the spirit of ‘Actions Speak Louder than Words’ [factum non verbum].” ) Introduction of Tsinghua University, http://www.tsinghua.edu.cn/eng/about.jsp?boardid=32&bid2=3201 (last visited on September 28, 2009).
focal points are dynamic, then the “nature and place” of use factor also counsels that a specially tailored and proportionate common remedy is in order, to fit the remedy to the offense.

4. The Fourth Step: a Common Remedy (integrating with other mark-related law)

The common remedy for focal point offenses in cyberspace is tailored. It is limited, proportionate to the harm, and graduated. It explicitly takes the public interest into account before considering injunctive relief, so it explicitly embraces the eBay\textsuperscript{137} principle of non-automatic prohibitory injunctions in patent and, by extension, in other intellectual property cases.\textsuperscript{138} The remedy is “common” because it is proposed to be applied to all focal point offenses in cyberspace whether arising under trademark law, unfair competition law, or any other cognate, including the statutory solutions for particularized offenses such as dilution offenses and cybersquatting offenses, and whether arising under contractually ordered dispute resolution policies, or otherwise.\textsuperscript{139} Because the remedy is the same and is proportionate in all circumstances, there is both an immediate simplification and clarification of the law, and also less pressure upon juridical actors to find the right label, or “cause of action.”\textsuperscript{140}

The common remedy includes one or more of a technologically reasonable, and technologically effective: (a) disclaimer,\textsuperscript{141} (b) notice,\textsuperscript{142} (c) redirect,\textsuperscript{143} (d) release,\textsuperscript{144} (e) reciprocal auction,\textsuperscript{145} and/or (f) opt-out/opt-in.\textsuperscript{146} It may also include

\begin{enumerate}
\item \textsuperscript{137} eBay, Inc. v. MercExchange, L.L.C., 547 U.S. 388 (2006).
\item \textsuperscript{138} See Folsom, Embracing eBay supra note 18 (generalizing the holding that ordinary principles of equity apply in patent cases and recommending extension beyond patent infringement cases to a broader range of IP-related cases). Trademark injunctive remedies have always been rooted in equitable principles. Folsom, Missing the Mark supra note 16 at 157-59; see Restatement supra note 57 at §35.
\item \textsuperscript{139} See infra footnotes 170-173 (providing references to some of those other offenses outside of trademark law).
\item \textsuperscript{140} “The causes of action we have buried, but they still rule us from their graves.” F. W. Maitland, The Forms of Action at Common Law 1 (Cambridge 1971) (1909). Who’d have thought that, when dealing with new technological uses in the code world, in the 21st century, we would still be struggling with such issues as whether to call it a trademark offense, or something else? If the focal point offense is actionable, then let it be actionable, and with the same core remedies regardless of packaging or form of pleading. Of course, if the focal point offense is compounded by independently actionable trademark-related wrongs, then any independently appropriate remedy may be added. But the core, common remedy is the basic starting point.
\item \textsuperscript{141} The disclaimer is a statement that the location is not associated with, sponsored by or affiliated with a mark proprietor.
\item \textsuperscript{142} A notice is an expression which includes the address or other addressable location of the mark proprietor. It might take the form, on the telephone side of cyberspace: “you may reach Holiday Inns by dialing 1-800-HOLIDAY, making sure to dial the number ‘6’ for the letter ‘O’ and being sure not to accidentally dial the number ‘zero’ as you just now did.” See section II infra (solving the Holiday Inns case, as a focal point offense).
\item \textsuperscript{143} A redirect is a coded expression which will actually deliver the user to the location of the mark proprietor. It might take the form, on the world wide web side of cyberspace: “you may click [here] to go to the web site of the software company that has registered ‘MOIVEBUFF’ as a trademark for high-end professional-grade databases about motion pictures.” See section II infra (solving the Brookfield case, as a focal point offense).
\item \textsuperscript{144} A forced release (or forced redirect) actually delivers the user to the desired location, or at least breaks the connection and forces the user to select a destination, but with a fair choice. It might take the form, on the telephone side of cyberspace: “you have certainly misdialed, and you certainly intended to reach Holiday Inns, please copy down these two phone numbers [one of which is 1-800-465-4329 for Holiday Inns, and the other of which is a “clean” 800 number for the competing reservation broker, having nothing to do with Holiday Inn’s number] this call will automatically terminate and you will have to redial, either us or them. Press # if you want to hear this message again.” See section II infra (solving the Holiday Inns case, as a focal point offense).
\item \textsuperscript{145} A reciprocal auction might put the associative focal point up for bid to that relatively small set of users who might have an association with it, but with the understanding that the “winner” might be expected to include
(g) prophylactic and compensatory measures including an award of reasonable attorneys’ fees, especially if the offending user has been asked by a mark proprietor and has refused voluntarily to provide a reasonable technological accommodation (I refer to this request-response cycle as “polling” or “sampling.”). The same technology enabling code to capture focal points also enables actual, effective, and efficient remediation by recoding to remove the harm, and precisely the harm caused by their misuse. The remediation can, by the power of code, occur prospectively at the point of harm and can preserve the sovereignty of the user’s choice and the robust nature of cyberspace signaling.

5. The Fifth Step: The New Nature and Place of Use Factor (for likelihood of confusion)

The prior Articles claim a new factor: the “nature and place of use” can resolve the characteristic problems of trademark infringement by assessing likelihood of confusion in cyberspace. The new likelihood of confusion factor can be fully specified for rule-based application to the paradigmatic cases in space.

Whether an actor’s use of a designation by an invisible or attenuated cyberspace intervention causes a likelihood of confusion with the mark of another is determined by considering all of the relevant factors, including:

(a) the nature of the cyberspace intervention, including the nature of the offending party and the nature of the supposed victim,

(b) the place of use and degree it implicates foundational cyberspace values,
(c) the presence or absence of any other relevant “ordinary” trademark likelihood of confusion factor or related factors from cognate laws or authoritative norms, 155

(d) the presence or absence of real-time sampling (or polling) 156 and any other relevant circumstances including tampering, spoofing, ambushing, or spoiling, 157 and

(e) an explicit assessment of the public interest in a robust and freely navigable cyberspace both at the liability stage and at the limited common remedy stage. 158

Unless accompanied by other circumstances, an invisible or attenuated likelihood of confusion in cyberspace is subject only to the limited common remedy, and not to the ordinary battery of trademark infringement remedies.

The fully specified factor recaptures, in element (e), a concern for the public interest in navigating cyberspace, and it expressly incorporates a limited, graduated and proportional remedy taking the public interest into account for purposes of assessing potential trademark infringement or cognate offenses. 159 The new factor can be stated in a rule-specific form, definite enough for ex ante planning, ex post adjudication, and all points in between.

Perhaps equally, if not more significant, is its recapture, in elements (a) through (d), of the surprisingly missing factual inquiry: where is the credible evidence of likelihood of confusion? When focal point offenses in cyberspace are clumsily addressed by currently existing legal tools, one of the oddest and least-remarked upon problems is the thinness of rational fact-finding. 160 Does a focal ordinary space, such as a purchase transaction executed over the phone or on the Internet not unlike it might have been executed in person or by mail order. Or it might involve cyberspace in a higher degree, as it implicates transactions not possible or at all, or only vaguely conceivable in ordinary space.

155 The new factor is intended to fit within every one of the various likelihood of confusion factor lists, each of which is careful to point out it is not exclusive. By the same token, the new factor does not displace any other likelihood of confusion factor which might continue to be relevant in considering invisible, expropriating and attenuated uses in cyberspace. Likewise, the new factor is intended to work in concert with cognate factor lists in the Anti-cybersquatting Consumer Protection Act (ACPA), Uniform Dispute Resolution Procedures (UDRP) or proposed Uniform Rapid Suspension System (URS) in ICANN-affiliated transactions, dilution factor lists, and other mechanisms. See infra footnotes 170-173 (providing references) and section __ infra (making more detailed application). The new factor is comprehensive and permits juridical agents to consolidate the various factor lists, abstracting from each of them concrete examples of conduct which might be relevant to consider in assessing likelihood of confusion, thereby unifying the various mark-related standards in cyberspace.

156 See text at note 163 infra (providing further details); and see Folsom, Space Pirates, supra note 17 at 893-94 (explaining: “Polling” is a query made at or near the point of the cyberspace offense, coupled with a request for voluntary implementation of reasonable technological accommodations); Folsom, Non-Neutral Principles supra note 18 at 94-100 (extending the analysis and recommending a form of polling, by tendering an offer of a reasonable technological accommodation, as a highly relevant factor in deciding whether to impose secondary liability arising out of new technological uses).

157 The nesting of the focal point offense elements within the new trademark likelihood of confusion factor is no accident, but is intended to unify the treatment regardless of label.

158 The inclusion here of an assessment of the public interest at both the liability stage and at the remedy stage is not an accident, but is intended to reinforce the essential importance of the graduated and proportionate remedy.

159 The Supreme Court has recently reminded courts to consider all of the equitable principles including an explicit consideration of the public interest prior to issuing injunctive relief that excludes others from competing. eBay, Inc. v. MercExchange, L.L.C., 547 U.S. 388 (2006).

160 Cf. generally, Graeme B. Dinwoodie [pick one] (reiterating the desirability of not merely designating the appropriate “test” for determining trademark-related disputes, but also the practical necessity of thinking about meaningful evidence that might contribute to a sensible application of any test); but see Daniel M. McClure,
point lead to some initial interest? Well, sure, what else would it do? Does this constitute a likelihood of confusion? This is the question to be answered, yet case after case seems based upon some one or more question-begging exercises in the unhelpful quagmire of imponderable, ineffable, and indemonstrable notions surrounding the current inquiry into “likelihood of confusion” caused by invisible or attenuated marks in cyberspace.

One of many helpful consequences of the new focal point offense coupled with the new “nature and place of use” likelihood of confusion factor is the recovery of the rational factual inquiry that has long been part of any adjudication of liability predicated upon a rule of law.

In its ability to capture readily available, highly relevant evidence “sampling” or “polling” is an especially interesting concept, and one that takes advantage of coded responses available in cyberspace. By constructed code, it would be possible to query in at least three directions:

A first query, simplified for this example, may be addressed by a mark proprietor to the focal point actor: “you are using my mark as a focal point in cyberspace, will you please add [one of the common remedies]?”

A second query, simplified for this example, could be addressed to a resource provider who might possibly be secondarily liable:

I have become aware of [some focal point offense] involving one of my marks for which you might be secondarily liable. Will you implement a reasonable technological accommodation, with my assistance and with my contribution to the costs, to reduce or eliminate the offending actions?

A third query—perhaps the most important of them all—simplified for this example, may be addressed by the focal point actor to the person drawn by the focal point (the alleged “victim”), effective and operative at the point of action:

“you have been pulled to this location because you entered ‘TRADEMARK’ but this particular location is not owned by, sponsored by, or affiliated with the mark proprietor, but by me—click [here] if you wish to continue with me, click [there] if you wish to be redirected to one or more mark proprietors.”

The responses to these queries by any of the various polled or sampled should be highly relevant in determining whether there is a likelihood of confusion. The third query, in particular, avoids problems of hindsight reconstruction and provides a relatively clean an ex ante determination of both subjective intent and objective effect. According to the first and second queries, the offer, or refusal to offer such

---

161 “We shall grapple with the ineffable, and see if we may not eff it after all.” DOUGLAS ADAMS, DIRK GENTLY’S HOLISTIC DETECTIVE AGENCY, ___ (1987). It may very well be time, finally, to “eff” the ineffable and actually to designate some factors appropriate for cyberspace and which are actually susceptible of real proof, rather than simple speculation.

162 See section II infra, solving the inapt application of current likelihood of confusion factors as one additional advantage of the “nature and place of use” factor.

163 “Sampling” or “polling” is inherent in the focal point offense and it is an explicit factor as part of element “d” in the newly proposed likelihood of confusion test.
sampling or polling at the point of asserted confusion isolates, identifies, and separates pirates and predators from value-adding or innocuous bystanders or users. Recalling the Pareto-optimal solution to the poisoned flower example, it would seem the only person in Martha’s position who would refuse such accommodations is a person who has no legitimate reason to persist in her offensive conduct—someone who either intends to kill dogs or doesn’t care if she does.

C. Summary

The focal point offense. In an objective cyberspace which relies upon a virtual map characterized by dynamic focal points functioning as markers, addresses or magnets, any conduct that (1) alters or tampers with the virtual map, (2) plants deceptive focal points, (3) ambushes or deluges a user of focal points with uninvited or false invitations, or (4) expropriates, blocks or spoils focal points otherwise available, thereby denying access, obstructing navigation, diverting traffic, taking advantage of augmented presences, or destroying trust in cyberspace, is an actionable focal point offense.

Residual cases of likelihood of confusion. The focal point offense includes all cases employing trademarks as focal points,164 and so resolves all of them. For those residual cases in which the mark proprietor cares to pursue trademark infringement as well, the “nature and place of use” factor determines whether conduct constituting a focal point offense might also constitute likelihood of confusion. The fully specified “nature and place of use” factor considers: (a) the nature of the conduct, the offending actor, and the supposed victim, (b) the place of use and the degree it implicates foundational cyberspace values, (c) the presence of any other “ordinary” trademark factor or relevant factors from cognate laws, (d) the presence of real-time sampling (or polling) and any other relevant circumstances including tampering, spoofing, ambushing, and spoiling, and (e) the public interest in a robust cyberspace.

The common remedy. Given a focal point offense, or a likelihood of confusion caused by an invisible, expropriating or attenuated use, the common remedy includes one or more of a technologically reasonable and effective: (a) disclaimer, (b) notice, (c) redirect, (d) release, (e) reciprocal auction, and (f) opt-out/opt-in, plus prophylactic measures and reasonable attorneys’ fees in appropriate cases. It should provide no more, and no less, than the minimum necessary to fit the remedy to the offense and preserve the public interest in a robust and freely navigable cyberspace.

The relationship between focal point offenses and trademark infringement. I claim there is a cyberspace focal point offense, apart from trademark law, which can be specified and should be recognized. When and if trademark infringement is

---

164 It includes all focal points and so it resolves more than the problems caused by that subset of focal points incorporating trademarks—it actually gets at the real problem: offending focal points that, in an analogy to the dead dog and the poisoned flowers that killed it is nonetheless wasteful, mean-spirited, and readily fixed. Like the poisoned flowers in cyberspace that might not constitute any nuisance under the rules of ordinary space, so also the deliberately offending, non-recorded focal points, including those which don’t contain any trademark at all, violate the public interest in cyberspace itself, forfeit any claim to legitimate use, and already constitute misappropriation or theft, fraud or deceit, or unfair competition.
asserted as a separate offense, then likelihood of confusion may be assessed according to a new “nature and place of use” factor analysis. The presumption is that the common remedy will ordinarily suffice under either theory, as long as the trademark offense is invisible and attenuated.\(^{165}\) If and to the extent the trademark offense in cyberspace is more than invisible and attenuated, and is simply an example of ordinary infringement transposed to space, then the ordinary battery of trademark remedies, including the prohibitory injunction, may apply. Much depends upon the circumstances: when the focal point offense and its harm are somewhat analogous to the *Shredded Wheat*\(^{166}\) or *Blinded Veterans*\(^{167}\) patterns, then the common remedy, analogous to the simple precautions in such cases, should resolve the conflict. But where the offense rises to a higher level so may the remedy.

If most, or a substantial plurality of attenuated and invisible uses in cyberspace should be resolved as focal point offenses, then there would be no need to proceed to the more expensive and time-consuming adjudication under the new “nature and place of use” analysis for likelihood of confusion in cyberspace, especially when the common remedy is the same under either theory. It is possible there might be yet another class of cases in which the mark proprietor is not satisfied with the common remedy.\(^{168}\) For that indeterminate (but perhaps quite small) last category, then the ordinary battery of trademark remedies would be available. It would seem that, apart from the few exceptions just noted, ordinary remedies would probably be reserved for cases of fairly straight-forward trademark infringement merely transposed to cyberspace.\(^{169}\)

*From trademark to focal points and back again.* I propose the common remedy to unify the treatment of related and cognate offenses including the UDRP,\(^{170}\) URS

---

\(^{165}\) See text at note 174 *infra* for an exception to this presumption.

\(^{166}\) *Kellogg Co. v. Nat’l Biscuit Co.*, 305 U.S. 111 (1938). This pattern obtains where there is an expression, like “shredded wheat” which has been determined to be generic, and hence incapable of legal protection as a trademark, but which might nonetheless be associated with a particular source. In these circumstances, a junior user may use the expression “shredded wheat” and may package the product in a box, and may decorate the packaging with artistic renditions of the biscuits in a bowl, drenched with milk, but must so display the competing product, market and differentiate it in such a way as to avoid deception, misappropriation, or other acts of unfair competition. *Id.* at __.

\(^{167}\) *Blinded Veterans Assn. v. Blinded American Veterans Found.*, 872 F.2d 1035 (D.C. Cir. 1989). Similar pattern, involving “Blinded American Veterans” and a junior user of a similar expression, with similar results: the junior user is required to use with care to avoid unfair competition. *Id.* at __.

\(^{168}\) This would include those cases in which there is true preclusion-style initial interest confusion, and perhaps some others. See ___ *infra* (giving examples of true preclusion-style initial interest confusion).

\(^{169}\) Not everything in cyberspace has to be special. Once code is used to create what reads like a magazine page, or displays as a film clip on the worldwide web, then it seems any “use” of an expression “as a mark in space, or in such a way as would cause a likelihood of confusion with the mark of another person really would be very nearly the same as any other conflict in ordinary space, to be resolved under ordinary principles of trademark-related law. It is when the special characteristics of cyberspace which feature and foster invisible and attenuated uses of expressions as dynamic focal points, some of which incorporate trademarked expressions, interrupt ordinary normal relationships that obtain in ordinary space that something somewhat out of the ordinary is needed. My approach is intended always to concentrate on what is actually happening and to apply the corresponding rule and remedy. Finally, my approach is modest in relation to my own limitations as a law professor. I cannot now imagine all the cases that might arise, and I do not exclude the possibility that there might actually be some case in which some circumstances might justify a remedy for an attenuated likelihood of confusion caused by an invisible or attenuated use greater than offered by the common remedy. I can’t think of any such case, but I do not exclude it. Hence I leave my proposal open to such a thing, at least for now. See text at note 174 *infra*.

\(^{170}\) “UDRP” refers to the Uniform Dispute Resolution Procedures. Internet Corporation for Assigned
and other suggested proposals,\textsuperscript{171} ACPA,\textsuperscript{172} and dilution offenses,\textsuperscript{173} and to anticipate changing technologies so there will be no need to create a new statutory, regulatory, or contractually-defined offense for each new technological use involving trademarks. But most importantly, my goal is to design rules that are calculated to preserve the public interest in a robust and freely navigable cyberspace. This has led me to focal point analysis, which resolves the greater problem of which existing trademark and trademark-related law is merely a distracting subset. I propose rather than starting with trademark infringement analysis when confronted with offending dynamic focal points, we should start with the focal point offenses and resolve them according to the common remedy. After resolving the focal point issues, and in residual cases in which the proprietor might want to assert trademark infringement for additional trademark remedies beyond those provided by the common remedy, we would employ the new “nature and place of use” factor to resolve the question of likelihood of confusion.\textsuperscript{174}

II. APPLYING THE NEW SOLUTION: IT WORKS

The second claim is that the new factor (as a comprehensive solution unifying the focal point offense, trademark likelihood of confusion factors and other mark-related regulations) works: it can resolve cases while avoiding or dramatically minimizing the risk of spectacular error. The new factor will be tested against illustrative examples, against representative leading cases, and against potential disasters waiting in ambush.

These illustrations are given in a spirit of cooperative inquiry and more fully to flesh out the nature of the new factor. They are also given in perhaps more detail than necessary. Once the reader gets the knack, all the illustrations resolve in very nearly the same way, with variations primarily at the level of the common remedy. After having read some of the illustrations, a reader might skip to Section III, perhaps skimming this section simply to see how easily the focal point offense works. Indeed, I envision a reader who might well have wished for more than can be done within the scope of this Article—who might be impatient with the apparent limitation that we are still dwelling, as it were, in the archaic techno-dust of the late-twentieth century. Would that we could indulge such a reader by giving illustrations such as these:

Names and Numbers (ICANN), Uniform Domain Name Dispute Resolution Policy (UDRP) (as approved by ICANN on Oct. 24, 1999), http://icann.org/dndr/udrp/policy.htm.

\textsuperscript{171} “URS” refers to the proposed Uniform Rapid Suspension System. ICANN, Implementation Recommendation Team (IRT) Report (May 29, 2009) at 25-37, http://www.icann.org/en/topics/new-gtlds/irt-final-report-trademark-protection-29may09-en.pdf. There is some fluidity, and other proposals are being floated for consideration [____]. [add ICANN’s proposal, as refined per draft 3, and as currently tabled indefinitely (check & update prior to publication)].


\textsuperscript{174} This makes room for the (currently unanticipated) category to which I refer in the last two sentences of footnote 169, supra.
(a) “the actor intercepts signals emanating from a nanotech medical device implanted in another person and inserts code…”;  
(b) “the actor thinks it would be fun or profitable to break the encrypted code of a bank account, or the commercial electronic funds transfer system (the so-called wire transfer system), or a remotely controlled military weapon…”;  
(c) “in a time when there are logo-bearing garments, road signs, and commercial signage illuminated by embedded LED-like devices, the actor flips the electronic switches so that the logos, directional and warning signs, and commercial signage display different messages, as the actor pleases…”;  
(d) “in a virtual world, the actor inserts disruptive code which terminates avatars, defaces the aesthetics, loots virtual property, or counterfeits virtual money for use as a medium of exchange in ordinary space regardless whether such conduct violates the terms of any end user license agreements and regardless whether any other player is in “privity” of contract…”;

175 This is a problem in psiberspace, beyond the primary scope of this Article. See text at note 207 infra (giving, in illustration __, an example that incorporates a trademark).

176 Many examples could be given, but in honor of the provenance of the word, “cyberspace,” see William Gibson, Burning Chrome (1984) (recounting an intrusion which “burned” the bank account of Ms. Chrome).

177 These are problems in cipherspace, beyond the primary scope of this Article. See AMERICAN LAW INSTITUTE & NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAW, UNIFORM COMMERCIAL CODE (official ed. 2009), §4A-203(a)(2) (placing the risk of loss of a fraudulent electronic funds (wire) transfer on a bank based on the assumption that the encrypted code of a “reasonable security procedure” is unbreakable without the cooperation of an inside source); id. cmt. 5 (“Breach of a commercially reasonable security procedure requires that the person committing the fraud have knowledge of how the procedure works and knowledge of codes, indentifying devices, and the like… This confidential information must be obtained either from a source controlled by the customer or from a source controlled by the receiving bank.”); but see RSA Laboratories, Public Key Cryptography Standards: What is a one-way function?, http://www.rsa.com/rsalabs/node.asp?id=2188 (last visited on November 14, 2009) (warning: All practical public-key cryptosystems are based on functions that are believed to be one-way, but no function has been proven to be so. This means that it is theoretically possible to discover algorithms that can compute the inverse easily [and without the need to have the privately-held key to the “back door”]… this development would render any cryptosystem based on these one-way functions insecure and useless.”) (emphasis added)

178 and cf., e.g., Siobhan Gorman & Evan Perez, FBI Probes Hack at Citibank, Russian Cyber Gang Suspected of Stealing Tens of Millions; Bank Denies Breach, WALL ST. J., December 22, 2009 (reporting that “[i]t couldn’t be learned whether the thieves gained access… directly or through third parties” and that the Bank has asserted “Allegations of a breach [or our] systems and associated losses are false.”) (emphasis added); Siobhan Gorman, Yochi J. Dreazen & August Cole, Insurgents Hack U.S. Drones, WALL ST. J., December 17, 2009 (describing intercepts of unencrypted code generated by an armed weapon system in flight).

179 These are problems in the metaverse, beyond the primary scope of this Article. The examples given here are based on the programmable "loglos" (presumably, logos that glow) envisioned in the metaverse created, so far, only in fiction. NEAL STEPHENSON, SNOW CRASH (1993).

180 These constitute further problems in the metaverse, beyond the primary scope of this Article. In fact, the proposed solution to the Martha-Dank poisoned flowers problem, while almost certainly correct, is not immediately self-evident: why did not Dank simply reconstruct a dog, or create a method for his dog to identify and to reject flowers, and why did the creator/proprietor of the virtual world not intervene at Dank’s request? There are answers, to be sure, and the proposed solution almost certainly presumes a certain set of parameters in this particular coded environment that limit Dank’s ability to create his own classes or objects with inheritable methods, properties or functions that Dank can extend (perhaps he’d have to replace each sophisticated or “trained” dog with a new dog having certain primitive methods, he has to “level up” to increase them, and there is no pre-formed “level” that constitutes “poison-immune.”) and perhaps it is better to leave the world-proprietor out of it, if possible. See, e.g., Joshua Fairfield, Anti-Social Contracts: The Contractual Governance of Virtual Worlds, 53 MCGILL L.J. __ (2008) (demonstrating the inadequacy of ordinary, untransformed, contract law to provide for all the needs of the virtual community); Mark Bartholomew, Advertising in the Garden of Eden, 55 BUFF. L.REV. 737 (2007) (proposing zones of exclusion in virtual worlds, where all advertising would be prohibited). [cite to Professor Lee (?)]
(c) “in a coded world, it is possible to read in a first jurisdiction text created in a second jurisdiction; and the libel law in a first jurisdiction either does not recognize truth as a defense, or puts the burden of proving truth on the defendant, thereby exposing an actor to legal liability in the first jurisdiction according to what is characterized as ordinary territoriality principles extended into the code world…”

(intervening illustrations ζ–ψ omitted); …

(ω) “the government, or any other actor, uses code to search for and to watch other persons, monitoring their movement, action, and history, and keeping a comprehensive profile-inventory, and perhaps in such a way as not to be noticed by the targeted person…”

And we might also include the corresponding problems of secondary liability throughout the code world.

Those extended illustrations must wait for another day, and I trust the reader will be content with the more mundane examples to be provided, and limited to the topic of this paper: mark-related conflicts in cyberspace. While I claim that the same method which solves the problem of marks in space can also be adapted to address the problems elsewhere in the code world, it should be tested on a smaller scale first. Accordingly, it is best to stay limited in scope, and to demonstrate initially that we can actually solve one kind of problem before advancing to so many others.

The distinctive values of cyberspace are access, navigation, information activity, augmentation, and trust. A trustworthy map of cyberspace relies upon navigational markers, and upon new machines that can find them, interpret them, and direct traffic towards them. The actionable marker or spoiler offense is a focal point offense. It might also be called a “cyberspace intervention” or invasion using

---

180 These are problems in the blogosphere, beyond the primary scope of this Article. See, e.g., L. Gordon Crovitz, A Town Called Sue, WALL ST. J. A19 (Dec. 21, 2009) (observing that lawyers “now joke that London has become ‘A Town Called Sue.’ Litigants may have only a most tenuous connection to England.”) The English laws may be about to change, id., but in the meantime and “[a]s one critic put it, ‘An English scientist [or could be an Icelandic academic, a Ukrainian-based online news site, or an American author] gives an interview in America to a Canadian journalist and an American online magazine about an American company and ends up getting sued in London. If he loses he will be bankrupt.’” Id.

181 This includes the public law/privacy and Fourth Amendment issues identified by Professor Lessig, but beyond the primary scope of this Article. See LESSIG, supra note 1 at __ (reexamining the telephone wiretap cases in the context of cyber searches and underlying principles). [add the recent W.St.J. accounts of hacking into Google gmail accounts, including those of dissident Chinese nationals, possibly by or on behalf of the Chinese government].

182 Because it is possible for a resource provider to monitor by code, and to meter and apportion economic rents by code, then under “ordinary” principles of secondary liability, woodenly applied in the code world, it would seem that almost any resource provider (including those who provide checking accounts, credit cards and any other payment clearing systems) would necessarily enable or contribute to the wrongful conduct of the malefactor with specific “knowledge” of it, or would be in a relationship having an ability to control the malefactor and with a directly apportionable financial interest in the misconduct. Likewise, the inventors and distributors of new machines capable of monitoring their use could be secondarily liable. And yet such “hostage-style” liability would seem to be an unacceptable over-extension of liability. See Folsom, Non-Neutral Principles, supra note 18 text at n. 172 [check] (listing some of the adverse effects of such extended secondary liability in the code world).

183 There are many places within the code world. Cyberspace is but one of them, and mark-related conflicts in cyberspace is only one context. See footnote 112 supra, and see Appendix B (proposing a taxonomy of the code world, including the metaverse, psiberspace, cipherspace, and cyberspace proper.)
focal points. The actionable offense involves calculated misrepresentation or deception, misappropriation or theft, waste, spoilage or unfair competition in an objective cyberspace relying upon a virtual map characterized by trustworthy markers, addresses and magnets. This underlying cyberspace offense always involves markers or spoilers.

Accordingly, the deliberate placement of a deceptive marker is conduct already constituting an offensive use of the expression simply “as” a deceptive address or magnet (an offending marker). The marker offense may be compounded by its use in connection with marketing the offending actor’s goods or services in a way causing a likelihood of confusion with the trademark of another. Likewise, the deliberate use of an expression as a spoiler is already offensive conduct simply by use of the expression “as” a roadblock or detour (a spoiler). The spoiler offense may be compounded if its use prevents or substantially interferes with another person’s marketing, sponsorship or promotion of goods or services under its own trademark.

Such offending uses of markers and spoilers (as address, magnet, roadblock, or detour) may be in addition to, or instead of, any use of the offending designation “as” a mark visibly and immediately associated with the offending actor’s goods or services, and might not even be advertised or promoted as such by the offending actor. Instead, the associations may be invisible and attenuated. Many such uses are “invisible” to most ordinary human observers, but are machine readable. Many such uses are “attenuated” because, though separated from or only remotely connected to marketing, sponsorship or promotion, they are nonetheless tied by technological means to such ends. Some such uses are “expropriating” because they suck the goodwill out of a pre-existing mark by preventing or substantially interfering with the mark proprietor’s use of its own trademark.

These offending uses nonetheless constitute tangible cyberspace interventions in an objective cyberspace regardless whether they also constitute trademark infringement. The actors responsible for offensive interventions purposely place designations in an objective cyberspace where they act as “markers” or “spoilers” drawing, influencing, cluttering, diverting, ensnaring, or stopping traffic. Some illustrations will serve to show how easily the new factor resolves the cases of offending focal points.

Prior to considering the illustrations, it should be remarked there are different kinds of focal points: (1) inherent focal points, (2) associative focal points, and (3) focal points incorporating a trademark. An inherent (or natural) focal point is like “Eiffel tower.” It simply is either the best choice, or one of a limited number of very good choices. An associative focal point is one that gains salience from

---

184 If neither an ordinary person nor a machine could detect, interpret or be drawn to a magnet, it wouldn’t work as a magnet.

185 If the expression were not tied to such ends, it wouldn’t be a commercially significant magnet though it might still disrupt access, navigation and information-seeking activities, take advantage of augmented presences, and destroy trust.

186 If the expression did not block a mark proprietor from effective use of the mark, there would be no “after-market” in reselling such expressions back to the mark proprietor, nor any need for mark proprietors to engage in various uniform dispute resolution or like procedures.

187 See supra note 31 (illustrating the use of a focal point to solve the problem of where to meet in Paris).

188 As long as there is more than one reasonable guess there is, of course, no guarantee of the result. One
repeated use, from convention, or from some sort of “buzz,” promotion, “viral” propagation, or advertising.¹⁸⁹ Finally, an associative focal point incorporating a trademark or service mark (a mark) of another person is important enough to constitute its own subcategory.

The focal point that incorporates a mark can also be very like an associative focal point insofar as it gains its salience from the coincidence of the characteristic feature of any mark; it has been so used as to identify a product provider and to distinguish it from other providers.¹⁹⁰ And yet at the same time a focal point incorporating a mark can be very like an inherent focal point insofar as it is the best way to find a branded product, information about a branded product, a community of interest relating to a branded product, or to glean information about the class of products, including competing products, of which the branded product is one example. In such cases, it is often a consumer who elects to treat someone else’s mark as nominative term¹⁹¹ and thereby to use it as the best guess, or at least as a reasonable guess to search for products somehow like the trademarked product. When competitors, mappers and others place such focal points as addresses, magnets, markers or spoilers, they are not necessarily trading impermissibly on the goodwill of the mark provider. They may merely be answering the consumers’ reasonable desire for navigation in cyberspace.¹⁹² The response is not to bar such uses, but to rewrite the code to reopen the focal points for access and navigation, in accordance with the limited common remedy.

The goal of the focal point offense accompanied by a proportionate and graduated remedy is reasonably to regulate focal points without killing their use, on the one hand; and broadly to permit focal points without deluging the user with bogus and invasive trespasses on the other. The goal is not to shield any user from all inconvenience, but to protect the user from misrepresentation and fraud, misappropriation and theft, waste, spoilage and unfair competition; and to ferret out those cases also constituting trademark infringement. The greater interest being

or the other of the players may have guessed the Arc de Triomphe. In cyberspace and with dynamic focal points freely available there, a player may jump from one to the other.

¹⁸⁹ This usage may take liberties with game theory constructs, see supra note 95, but it provides clarity in the context of cyberspace.

¹⁹⁰ So if two were to meet for lunch in Paris, without more knowledge, then the Eiffel tower might be an inherent focal point. If at least one of them actually knew something about each other, as by prior association, then the better guess, and the better focal point solution, would be at a particular restaurant known to be a favorite because of its acquired game-significant meaning. A trademark is a paradigmatic associative focal point. It is both dangerous and desirable in cyberspace (not unlike the poisoned flower) because of the dynamic capacity of coded space.

¹⁹¹ This is a usage of an expression, by a consumer or other searcher, as if the trademark-containing search term were descriptive, or even generic according to the function that the consumer sovereignly decides to adopt at that moment. It is remarkable that this has nothing to do with the validity of the mark in respect of its inherent or acquired distinctiveness, but only with the use to which the consumer freely and in the absence of any discernable confusion elects to make of it. Likewise, this has nothing to do with any sort of privileged fair descriptive or nominative use defense, because consumers in this situation don’t cause a likelihood of confusion and so do not have to defend their own practices.

¹⁹² This, of course, is where the question of privileged comparative advertising, descriptive or nominative fair use would arise, because now there is a competitor or other offender, and other persons who might be secondarily liable for inducing or contributing to the offending conduct with knowledge of it. At this point, existing trademark likelihood of confusion analysis tends to break down because it lacks the tools to discriminate harmful and benign focal point activity from predatory and wasteful focal points, and it lacks a proportionate and graduated remedy to remediate any resulting harm to cyberspace by way of a reasonable technological accommodation.
served is the public interest in a robust, accessible, freely navigable, information-rich cyberspace which augmented presences may find trust-worthy enough to use.

A. Illustrations

I will provide illustrations under three headings: First, focal point offenses; second, residual trademark likelihood of confusion analyses; and third, related applications concerning secondary liability and other issues deserving of special treatment.

1. The Focal Point Offense

a. Altering the Map, or Planting Deceptive Markers—Dynamic Addresses as an historically important subset of markers in cyberspace.

A dynamic address is, among other things, an expression delivering an augmented presence to a place within cyberspace. Current law creates an economic rent in vanity addresses in cyberspace, making a market both in vanity phone numbers and vanity Internet addresses. Economic rent-seeking in dynamic addresses occurs because of the effectiveness of an address to deliver the augmented presences of persons seeking another person; a provider of goods, services or information; or a community of interest associated with the vanity address. There can be only a limited number of reasons for any address to have excess value attributed to its power to deliver traffic (wherein augmented presences are the “traffic”). Three of those reasons are: (1) the expression itself is an inherent focal point; (2) the expression is an associative focal point because it has been promoted or advertised in order to associate the expression with a person, goods, services, information, or a community of interest; or (3) the expression is a focal point incorporating a trademark.

Where the expression is itself an inherent focal point used to find something, it would seem to be a resource in the commons, but a special sort of resource. At one pole, such resources could go to the first appropriator. At the opposite pole, such resources could be shared and free to all, subject only to existing principles of ordinary law. Or (as I propose) such resources could be moderated by designed factors so as to function as focal points simultaneously open to any number of users, based on reasonable technological accommodations to ensure they continue to function as focal points.

Where the expression has been promoted or advertised as an associative address, it develops an acquired meaning because it leads to the associated place within cyberspace. As such it has become a focal point by acquired association, and is vested with all the concerns, interests and effects of any inherent focal point.

---

193 See text at note 185 supra (observing that a use is “attenuated” when separated from or only remotely connected to marketing, sponsorship or promotion of goods or services, but nonetheless tied by technological means to such ends).

194 Depending on context, the address is a notional location, it is a pointer to a coded place, and/or it is a coded place. My concern here is with what a dynamic address in cyberspace does. I am recommending that a law for cyberspace ought to be concerned about real relationships and need be concerned about the details of the code only when the details of the code makes a difference.
Like any other focal point, an associative focal point could be allocated to the one who created the association, it could become a shared resource free to all, or (as I propose) it could be moderated by reasonable technological accommodations.

Where the expression incorporates a trademark, it is a special case. The trademark in cyberspace is, in addition to whatever else it might be, a dynamic focal point. The trademark functions as an associative focal point in addition to whatever other function it might perform. The trademark aspects of the dynamic focal point assume a disproportionate impact because of two further concerns. First, trademark law is so firmly entrenched in “ordinary” law and so dominates thinking about cognate issues in cyberspace that it crowds out conversation about the obvious harms done by deceitful placement of markers as associative focal points, even where there is no likelihood of confusion. Second, trademark law is already so vulnerable to the abuses of doctrinal creep, reverse doctrinal creep, equivocation and “propertization” that any attempt to start a conversation about the harms of deceitful uses of associative markers, or focal points, quickly becomes caught in the trademark cross-fire.

A key to resolving the problems of addresses is to recognize they occur in cyberspace, cyberspace is code, code can be designed, written and rewritten, and the law may combine with norms, markets and architecture more nearly to choose a design of cyberspace to advance rather than retard the values of cyberspace. The way to encourage rewriting code is to require it as a reasonable technological accommodation. When I say “reasonable technological accommodation” I mean an accommodation that/rewrites the code to resolve the poisoned flower problem in cyberspace. This also contemplates the minimum reasonable accommodation sufficient to remedy the harm, measured in large part by the same technologies making the address effective to draw traffic in the first place, and it also means taking advantage of other technologies that come online afterwards. The focal point offense is designed deliberately to incorporate a common remedy which intentionally coincides with the technological accommodations necessary to preserve the functionality of dynamic focal points as aids to access, navigation, information-activity and trusted augmented presences in cyberspace.

I claim the new factor provides a rule of thumb (a heuristic) that actually moves cases along. It is practical, it works, and it turns formerly difficult cases into rather unremarkably (and almost boringly) similar patterns for resolution. These illustrations are intended to show the ease with which the new factor presses for a reasonable rewrite to the code. They are also intended to show the importance of a general law, regardless of the accidents of particular offenses, and particular search engine technology and user adeptness in “working around” invasive, deceitful and abusive cyberspace interventions. There is no need, no public interest, no natural right, no economic efficiency, and no sense in mistaking a love of liberty and of creativity in cyberspace, for an infatuation with mischief. There is no reason to privilege mischief that is deceitful, especially when there is a flexible remedy to ameliorate the harm while securing both liberty and the fundamental values of cyberspace.

At the outset, it might be objected that there is no direct precedent for such an action as here proposed. In the common catch phrase, a judge might well say
“plaintiff has not cited, nor has our own research been able to find a case on point.” The first illustration explains why there might be a dearth of precedent.

Illustration 1. Pineapple Inc., formerly incorporated as “Pineapple Computer, Inc.” has its principle place of business at 1 Recursive Loop, Cupertino, CA 95014 and has trademark rights in PINEAPPLE for computer software. A person not associated with Pineapple, Inc. purchases undeveloped property in Cupertino, obtains approval for a subdivision with a street designated “Recursive Drive” and a plat having the address “One Recursive Drive, Cupertino, CA 95014.” An actor not associated with Pineapple, Inc. incorporates a business as “Pineapp1e Computer, Inc.” (using the number “1” in place of the letter “L” in Pineapple, and adding the word which used to be in the company’s name) and takes office space at the address, One Recursive Drive, without any advertising or promotion of the fact. The actor receives a non-trivial amount of mail obviously intended for Pineapple, opens the mail and fulfills orders, cashes any included checks, provides tech support, discards some of the mail altogether, compiles lists of names which it sells to targeted advertisers and mail list aggregators, and forwards other pieces of mail to Pineapple, Inc. for a slight processing and handling fee. When confronted with allegations of fraud, mail fraud, theft, conversion and numerous other offenses, the actor asserts that it never “used” the expression “as” a trademark, that the expression isn’t identical to Pineapple’s, that Pineapple had failed and neglected to take office space at every conceivable address that might be a “trapping” address, and that the actor never advertised or promoted anything and never caused anyone to do anything, but rather simply happened to receive mail which the senders either misaddressed or which the post office misdelivered. The actor is liable under ordinary principles of law, under numerous theories including fraud, theft and ordinary trademark law likelihood of confusion.

I can’t say that illustration 1 is based on any case that has ever occurred in ordinary space. Therefore, it might truly be without precedent. But I think the reason it is unprecedented is not because the law fails to provide a remedy in such a case, but because the conduct is at the same time so outlandish, improbable, and difficult to accomplish on the one hand, and so obviously wrongful, illegal and easy to catch on the other hand, that no one would be so stupid as to make the attempt. If, however, anyone did engage in such conduct, it seems rather trivially obvious to assert there would be liability. I submit the reason there is no such precedent in ordinary space is that, at least in this regard, the reality of ordinary space is fundamentally different from the reality of cyberspace. I posit this example only as a sort of null” hypothesis set in ordinary space against which to compare the following illustrations drawn from cyberspace. The examples could be multiplied.\(^{195}\)

\(^{195}\) See infra, text at notes 126 - 129 (multiplying such examples), and see illustration 18 supra (semble).
i. Dynamic Addresses on the Telephone Side of Cyberspace

Consider vanity addresses on the telephone side of cyberspace. Within that group, consider an inherent telephone focal point: 1-800-LODGING (for hotel, motel or like services). Consider, next, but within the same telephone subset, an associative focal point: 1-800-MYHOTEL (notice “HOTEL” maps to only 5 places, and the conventional United States phone number requires two additional places to fill a string of 7 characters: the “guess” at filling the field with “MY” is not immediately intuitive, and would be substantially helped by the target-proprietor’s making known the code, “MY”—hence this is more nearly an associative than an inherent focal point).

Consider, finally, the yet more powerful associative focal point incorporating a trademark. Such a focal point may take the form 1-800-HOLIDAY. It can be immediately understood that the expression is a focal point, that it is an associative focal point for hotels, and that the association is powerful because it incorporates a shortened, but highly “guessable” form of a trademark owned by Holiday Inns, Inc. to signify its affiliated Holiday Inn hotels and related goods and services.

With those examples in mind, here are some illustrations:

Illustration 2. A first actor obtains and uses the phone number 1-800-LODGING in connection with goods or services related to hotel, motel or like services. A second actor obtains and uses 1-888-LODGING, and a third actor obtains and uses 1-877-LODGING in connection with similar goods or services. The expression LODGING is serving as an inherent focal point. Even if none of the users has any trademark rights in the expression “LODGING” a court may require each to provide a reasonable technological accommodation, including a notice, disclaimer or redirect. Each user making a reasonable technological accommodation may continue to use the expression.

Illustration 3. Same as illustration 2, except the first actor’s expression is 1-800-MYHOTEL, the first actor has taken steps to associate the expression with itself by advertising or promotion, and the second and third actors incorporate the MYHOTEL expression. The expression MYHOTEL is serving as an associative focal point. Same result as illustration 2, even if none of the users has any trademark rights in the

---

196 Others can be easily generated in the same vein. These include: 1-800-GLASSES (for lenses or frames, and vision services); 1-800-CONTACT (for contact lenses or vision services, or for ways to make some sort of “contact” with others); and 1-800-NEWYORK (for general goods or services originating from, or associated with a city).

197 Others can be readily surmised in the same fashion. Examples include: 1-800-GOHOTEL (again, this illustrates that as the fillers become harder to guess the need for an association correspondingly increases—here, the filler is “GO”); 1-800-99HOTEL (same, but here the filler is “99” and unless it were to become a convention, it would require some association before it can function as a viable, guessable, focal point); and 1-800-LETSKI (same, only now the key word is “ski” which uses only three of the seven positions) and so the filler requires a searcher to find 4 symbols and is more or less an effective associative focal point as these four become more or less “guessable,” aided by someone’s actually making some effort to publicize the association.
expression MYHOTEL. A court may select from the common remedy a technological accommodation proportionate to the harm, but each user making a reasonable technological accommodation may continue to use the expression.

Illustration 4. An actor not affiliated with Holiday Inns chooses the phone number 1-800-465-4329, which maps to 1-800-HOLIDAY, and then advertises and promotes the number and thereby attracts persons who have made the association and also persons who have simply guessed this was an address to reach Holiday Inns by phone (or to obtain associated goods, services or information, or to reach a community of interest). Notwithstanding that the expression HOLIDAY is a salient part of a trademark owned by Holiday Inns, this constitutes an independently actionable cyberspace intervention (a focal point offense) and from that perspective the actor may continue the use but a court may require a reasonable technological accommodation, including a disclaimer, probably coupled with a disconnect (a forced release) as a higher level of remediation. If this also constitutes an act of trademark infringement (see illustration 23A below) a court may also impose any other remedy from within the battery of trademark infringement remedies.

Illustration 4A. Same as illustration 4, but the actor chooses the phone number 1-800-405-4329, which maps to 1-800-H[zero]LIDAY and, without advertising its number, thereby traps persons who guessed 1-800-HOLIDAY was an address to reach Holiday Inns by phone but who predictably misdialed a “zero” for the letter “O” [missing the “6” which actually maps to the letter “O”]. Same result.

Illustration 4B. Same as illustration 4, but the actor chooses the phone number 1-800-465-1329 which maps to 1-800-HOL[one]DAY and thereby traps persons who guessed this was an address to reach Holiday Inns by phone and who predictably misdialed the number “1” for the letter “I” [missing the “4” which actually maps to the letter “I”]. Same result.

Illustration 5. Same as illustrations 4, 4A or 4B, but with full knowledge of the other users Holiday Inns or a person affiliated with it desires to promote the phone number 1-800-465-4329, which maps to 1-800-HOLIDAY (or any of the “trapping numbers” which is off by one or more characters in the string) but realizes these are already taken by another actor. Realizing that the other actors will have to provide a reasonable technological accommodation, including a notice or forced

---

198 Compare 1-800-465-4329 (reaching Holiday Inns or its sponsored site) with 1-800-405-4329 (trapping, as in this illustration 2, for persons trying to dial the Holiday Inns number but predictably misdialed “0” instead of “6” to get the letter “O” in “holiday”).

199 Compare 1-800-465-4329 (reaching Holiday Inns or its sponsored site) with 1-800-465-1329 (trapping, as in this illustration 3, for persons trying to dial the Holiday Inns number but predictably misdialed “1” instead of “4” to get the letter “I” in “holiday”).
redirect sending any caller to a “clean” number that would lead to Holiday Inns, Holiday Inns has no need to pay the actor, but may safely advertise and promote the vanity number incorporating a portion of its own trademark thereby ultimately attracting to itself the persons who have made the association and also persons who have simply guessed this was an address to reach Holiday Inns by phone. Upon a proper showing by any of the other actors that the actor has some connection to the expression embedded in the vanity phone number, the actor might be able to require Holiday Inns to include a reciprocal notice so that a caller would be able to choose which to call.

Illustrations 2-5 are based on Holiday Inns but with at least four significant changes in emphasis.

First, the facts that “LODGING” and “MYHOTEL” are not trademarks of anyone and that “HOLIDAY” is a trademark of Holiday Inns are not essential to the outcome. Likewise, the existence of advertising or promotion by the offending actor/proprietor of any of the vanity number is not essential to the outcome. The outcome depends upon whether the conduct is an actionable cyberspace intervention (a focal point offense), which depends upon whether and how it happens that the expression is a focal point, and what the allegedly offending actor is doing. In general, a focal point might represent a pure guess on the part of seekers, or it might have become an associative address because someone promoted the association. It might also function as an associative address because, as in illustration 4, it incorporates someone’s trademark.

Second, there are other persons who might have an interest in “lodging” or “myhotel” or even “holiday” as a focal point, and those include surfers, mappers (search engine providers and indexers), customers, consumers, and mark providers, and persons who enjoy, provide or are curious about “holidays.” The outcome does not turn upon whether any of those persons secured or failed to secure “trademark rights” in the focal points. It depends, rather, on the accuracy of the representation made in respect of the focal point and also upon the “appropriability” of the expression. This depends, in turn, upon the associative power of the address. The notion that, in the cases of illustration 4, 4A and 4B, some mark proprietor “should” have secured any of the focal points either directly as a phone number or indirectly “as” a trademark, much less every one of those focal points, plus all variations, modifications, misspellings, and all formatives having the same or a similar sight, sound or meaning, is no part of this analysis. The point is to prevent deceit and misrepresentation, not to prove who

---

200 Holiday Inns, Inc. v. 800 Reservation, Inc., 86 F.3d 619 (6th Cir. 1996).
201 How utterly strange it would be for a court to surmise that it might be prepared to protect 1-800-465-4329 as a trademark because it maps to 1-800-HOLIDAY, but that it cannot protect 1-800-405-4329 because Holiday Inns failed to purchase all the possible variations of “Holiday” from the phone company. It is as if someone might have declared open season on expressions which cause a likelihood of confusion with some mark, but which are not identical to the mark in question because the proprietor of the mark had failed to register every expression which might be similar to the mark in sight, sound or meaning. See ___ (noting that the court made precisely that point, and also made the observation that the offending conduct by which the offending party used the trapping expression in connection with marketing directly competing goods and services causing actual confusion nevertheless did not constitute the “use” of the trapping expression accompanied by advertising or
can game the system. The illustration involving a trademark, illustration 4, does not require the mark holder to preregister every cognate, trapping, or sound-alike expression in order to have focal point rights, but on the other hand, those rights are limited to the extent necessary to remove the focal point harm—multiple users may coexist in cyberspace as long as they take reasonable technological steps to permit free and effective access and navigation.

Third, this very simple approach leads to a uniform and modest remedy. These illustrations may or may not constitute an independent act of trademark infringement, and illustrations 2-3 certainly do not. But each is a focal point offense, and because of the common remedy, the stakes are not spectacular. It is neither a windfall to one, nor a disaster to the other party. The remedy suggested here offers the highest level of control at the point of a forced release (illustration 4), and that is not very intrusive at all. The outcome does not prevent the free and fair nominative use of the focal points, but only levels the playing field so users may continue to choose whether and where they will make a nominative use.

Fourth, we may move from the phone side of cyberspace to the worldwide web side (and to any other technology which should happen to arise in the future) without any new analysis. As long as the problem is the same—as long as it is a focal point offense—then the resolution is the same. The common remedy continues to resolve the common problem regardless of any particular technology in which the offense occurs.

ii. Dynamic Addresses on the Worldwide Web Side of Cyberspace

Here are some illustrations on the worldwide web side of cyberspace, all on the same principle as previously illustrated:

Illustration 6. An actor chooses a domain name which maps to lodgings.com. Another person chooses any one or more domain names which are identical in the second level (“lodgings”), but differ only in the top level—that is, lodgings.biz or lodgings.nu or lodgings.tv—or in insignificant changes at the second level, e.g., “lodging” instead of “lodgings.” Even if there is no trademark involved, if these are focal point offenses (depending on the strength and ubiquity of the gTLD [top level domains] other than the preferred/likely focal point “.com” domain, and as that strength might vary over time, or as the number of top levels may be expanded over time), a court may require one or both of the actors to make reasonable technological accommodations.

Many of the following illustrations are predicated on the historical happenstancce, and the implicit assumption that most persons searching for a dynamic address in a commercial context are likely to look for it in the “.com” gTLD. Those illustrations are not intended to be static. If, as, and when circumstances change, then so should the illustrations be adjusted to fit.
Illustration 7. An actor chooses the URL which maps to MOVIEBUFF.com thereby attracting a user who guessed, or a search engine which draws persons who guessed this was (i) an address or magnet leading to the provider who uses the expression “movie buff” (with a space between words) as a salient part of its common law trademark, or (ii) leading to the different provider who uses “moviebuff” (without a space) as the entirety of its federally registered mark, or (iii) to obtain associated goods, services or information, or to reach a community of interest. Regardless whether “moviebuff” or “movie buff” is a trademark, this is an independently actionable cyberspace intervention (a focal point offense). The actor may continue its use, but a court may require the actor to provide a reasonable technological accommodation such as a disclaimer with a redirect, and the court may require reciprocal notices if each party is related to the focal point.

Illustration 8. An actor chooses the URL which maps to FORD.com thereby attracting a user who guessed, or a search engine which draws persons who guessed this was an address or magnet to reach one of several providers who use the expression “Ford” or to obtain associated goods, services or information, or to reach a community of interest. Notwithstanding “Ford” is a trademark of several different proprietors, and in some contexts is not a mark at all, this is an actionable cyberspace intervention (a focal point offense). The actor may continue the use but a court may require the actor to provide a disclaimer with a redirect, or other appropriate remedy from the set of common remedies, including reciprocal notices.

Illustration 8A. Same as illustration 8, but the actor chooses one or more URLs from the set of URLs which map to FORD.org, FORD.nu, FORD.tv, FORD.car (among many others, and possibly including FORD.ford under some dramatically expanded gTLD system) thereby attracting a user who guessed, or a search engine which draws persons who guessed one of these was an address or magnet to reach one of several providers who use the expression “Ford” (or to obtain associated goods, services or information, or to reach a community of interest). Same result.

Illustration 9. An actor chooses the URL which maps to SUPERMAN.com thereby attracting a user who guessed, or a search engine which draws persons who guessed this was an address to reach one of several persons who use the expression “superman” including as a trademark (or to obtain associated goods, services or information, or to reach a community of interest). If this is an actionable cyberspace intervention (a focal point offense), the actor may continue the use but may be required to provide a reasonable technological accommodation, such as a disclaimer with a redirect.

Illustration 10. An actor places an address in any tangible medium of expression from which it can be perceived, reproduced or communicated in cyberspace either directly or with the aid of a machine or virtual machine now
known or hereafter developed. The expression functions as an address in cyberspace. If this is an actionable cyberspace intervention (a focal point offense), the actor may continue the use but may be required to provide a reasonable technological accommodation, such as a disclaimer with a redirect.

Illustration 11. A user is not entirely sure how to reach a particular person, or to how to find certain goods, services or information, or a community of interest, and the user initiates a search by launching an inquiry into a tangible medium of expression from which it can be perceived, reproduced or communicated in cyberspace either directly or with the aid of a machine or virtual machine. The inquiry is intended to retrieve an address in cyberspace. If the response to the inquiry, either directly or indirectly by the aid of a machine or virtual machine, constitutes an actionable cyberspace intervention (a focal point offense), the responder may continue its conduct but may be required to provide a reasonable technological accommodation, such as a disclaimer with a redirect, or a release. The user is neither a victim nor a wrong-doer. The responder’s legal status is independent of secondary liability, but is a direct application of the focal point offense coupled with its limited common remedy.

Illustration 12. In any of illustrations 6-11, a mark proprietor seeks to promote a focal point incorporating its own mark, but realizes the preferred focal point (or one or more other focal points that act as magnets attracting searchers for the mark) is already taken by another actor (or by more than one actor). Realizing that the actor(s) will have to provide a reasonable technological accommodation, including a notice directing any visitor to a “clean” location, or a redirect sending the visitor to the mark proprietor, the proprietor has no need to pay the actor(s), but may safely advertise and promote its own mark thereby ultimately attracting to its location the persons who have made the association and also persons who have simply guessed this was an address to reach the proprietor. Upon a proper showing by any of the actor(s) that the actor has some connection to the expression embedded in the focal, the actor might be able to require the proprietor to include a reciprocal notice so that a visitor would be able to choose which to visit.

These illustrations 6-12 are routine when they are treated as focal point offenses. All they do is take vanity phone numbers and extend the analysis to vanity domain names. Whether we are dealing with the historical epoch in which there were only seven gTLD’s and a number of country codes (illustrations 6 and 8A), or the modest expansion, or the promised infinite multiplication of gTLDs, the solution becomes trivially easy. These are all focal points, and some are associative focal points containing trademarks. Accordingly, each is a focal point offense easily resolved by modest technologically effective and technologically reasonable accommodations. The mark proprietor need not monitor, register, pay for, docket and renew, each of seven gTLDs, plus a number of the more important country codes, much less a near-infinite number of gTLDs that are on the horizon, plus all the trapping versions of each, and it would be perverse to require it. The
existence of the common remedy requiring redirects and releases, and reciprocal auctions will itself knock the arbitrage opportunities out of the game, leaving the addresses as operative focal points, leading to mark proprietors even as they might be used simultaneously by others who might thereby offer some value to users who navigate to them. If and when the technologies or techniques of addressing change, the same analysis will still cover the new techniques because the focal point analysis is not tied to any particular technology.

b. Altering the Map, or Planting Deceptive Markers—Invisible or Attenuated Uses (Magnets and Markers)\textsuperscript{202}

Consider that a vanity phone number or vanity domain name is often visible as an address, and is a dynamic focal point of one kind (per illustrations 2-12 above). Other dynamic focal points are not so directly operative as a visible address, but nonetheless pull or attract a search engine. This category includes conduct that alters the map, and in which a focal point functions as a marker or as a magnet, often invisible to the user.\textsuperscript{203}

Illustration 13. An actor places an expression in a tangible medium of expression from which it can be perceived, reproduced or communicated in cyberspace either directly or with the aid of a machine or virtual machine now known or hereafter developed. The expression functions as a magnet in cyberspace. Even if this is an actionable cyberspace intervention (a focal point offense), the actor may continue the use but may be required to provide a disclaimer with a redirect, or other reasonable technological accommodation.

Illustration 13A. An actor in the business of renting videos under the slogan “the video buff’s video store” places “video buff” (and “videobuff”) as a magnet, perhaps in hidden text or in coded expressions usually unseen by ordinary persons and hence “invisible” to them but able to attract a machine within cyberspace. Another person subsequently decides to register a trademark on the expression “videobuff” for high-end video data base products and after obtaining a registration, objects to the actor’s prior use of “videobuff” as a magnet. Even if the actor’s use of “videobuff” is an actionable cyberspace intervention (a focal point offense), the actor may continue the use but may be required to provide a notice, disclaimer and/or a redirect. Upon a showing of a focal point connection in the actor, a court may require a reciprocal response

\textsuperscript{202} See text at note 184 and __ supra (observing that a use is “invisible” when not readily perceptible to ordinary human observers, but is machine readable and “attenuated” when not immediately and directly associated with the marketing of related goods or services).

\textsuperscript{203} The focal point offense deals with dynamic focal points I’ve characterized, for ease of discussion, as addresses or magnets (markers). In a sense, every dynamic focal point is a magnet, and I don’t mind if someone should think of addresses as merely a species of magnet. But because of the accidental development of technology and commerce related to vanity addresses, and of the corresponding case law that developed in concert with the technology, it seems appropriate to discuss the “address” (which is something visible to many users, but often “attenuated” when considered under existing standards of trademark law) as a conceptual category apart from the “magnet” (which is something more often “invisible” to many users, and which may or may not be “attenuated” when considered according to existing standards of trademark law). Both addresses and magnets are “markers.”
by the other person.

Illustration 13B. Same as illustration 13A, but the actor incorporates “videobuff” within an address such as “videobuff.com” which may be entered by ordinary persons into a search engine, as a search term other than as an “address,” and which is also able to attract a machine within cyberspace. Same result (and see illustration 7).

Illustration 14. An actor sets a spider, or otherwise monitors expressions which serve as magnets in cyberspace and provides resources (for example, a list of address, ranked in presumptive order of interest to a user, or a set of trigger words offered for sale to various persons) by which others might be able to find, or be drawn to, those magnets. Some magnets incorporate inherent focal points, others incorporate associative focal points, and yet others incorporate focal points including trademarks (collectively, potentially actionable cyberspace interventions—focal point offenses—by third parties). Because of the power of code, the actor knows or could have known, monitors and controls or could have monitored and controlled; the actor materially contributes to, or induces the conduct; or (because of the power of code to allocate transactions) has a direct financial interest in the third party’s potentially actionable cyberspace intervention. Even where the third party’s conduct is an actionable cyberspace intervention, and even where the actor is secondarily liable to some claimant for the third party’s conduct under applicable principles of secondary liability, the actor may continue to provide the resources but may be required to demand that the third party actor provide an effective notice, disclaimer, opt-out, or other reasonable technological accommodations. If reasonably possible, and if the third party actors refuse, the actor may insert or be required to insert code which forces the desired result and a court may condition its award upon the claimant’s agreement to pay or share the costs of the actor’s reasonable technological accommodations, ensuring that the claimant is not opportunistically off-loading its cost of enforcement upon the actor.

Illustration 14A. Same as illustration 14, but the actor monitors addresses as well as markers and provides resources based on such addresses. Same result.

Illustration 15. Same as illustrations 14 and 14A, but the actor finds some way to sell or otherwise profit from its services, either by advertising, or by a user fee, or by cross selling or promoting some other product, or by otherwise benefitting from the third party conduct. Same result. The claimant is not entitled to share those fees or revenues, but a court may consider them in apportioning the share of remediation costs between actor and claimant.

Illustration 16. A user purposefully frames an inquiry to find something in cyberspace, deliberately using one or more inherent focal points, associative
focal points, or associative focal points that incorporate a trademark. The user could care less whether anyone has any rights in any of these expressions, and is not at all confused. The user is privileged to do whatever the user pleases, providing the user does not engage in an actionable cyberspace intervention (a focal point offense). Even if the user does engage in a focal point offense, there might be no judicial remedy, or a remedy might be fashioned if it can be done without prejudice to the interests of others in a robust and freely navigable cyberspace. If this is a substantial non-infringing use, other actors may cooperate with the user in providing navigational focal points. If any of this conduct constitutes a focal point offense, the actors’ liability (including direct or secondary liability) is limited as in illustrations 14 and 15.

These illustrations all involve invisible or attenuated uses of focal points and some of them involve secondary liability. If treated as cases of trademark infringement, they can be perplexing. But once they are analyzed as focal point offenses, they are routinely resolved by the rule of thumb which assigns a graduated and common remedy to each. The focal point offense reduces the jackpot-hostage risks, and readjusts the self-proving, question-begging nature of secondary liability as it currently is applied in cases of new technological uses.

c. Ambushing and Expropriating Uses (Spoilers, Detours and Roadblocks)

In cyberspace, it is possible to ensnare or ambush a user by providing uninvited or false invitations. It is also possible to warehouse, hoard, or officiously to become (as it were) a forced broker in respect of focal points. As at the outset, and as in the case of illustration 1, I will begin with an attempt to create a similar offense in ordinary space.

Illustration 17. A person is engaged in conversation on a public street while walking to her office. An actor overhears her and recognizes that she has uttered a focal point. The actor follows her, all the while speaking to her, repeating the focal point, giving her information about the focal point and things related to it, advising her how to get to the focal point, what to do with the focal point, and where to find other goods, services, places or communities

---

204 See Folsom, Non-Neutral Principles, supra note 18, passim and especially text at note 172 (explaining in more detail: since code can control or supervise, and does materially aid (and its proprietors often promote, encourage and induce its use), and may meter or allocate the direct benefits of the conduct, there is a natural pressure to conclude that all providers of such resources must intrusively monitor on penalty of potential secondarily liable for the primary offenses that occur). That would be a bad result, and should be resisted. Id. My approach dramatically reduces a resource provider’s exposure to ruinous or technology-stopping secondary liability.

205 See text at note 186 supra (observing that a use is expropriating when it deprives a mark proprietor of the opportunity effectively to work its mark by preventing or substantially interfering with another person’s marketing, sponsorship or promotion of goods or services under its own trademark). This is a signature offense in cyberspace.

206 Examples can be multiplied. Suppose there were an interstate highway system, but with centralized regulation billboards such that only one unique billboard could answer to any one unique focal point, and that billboards were allocated on a first-come, first-served basis. Then we would have been confronted with the phenomena of artificially induced scarcity of focal points and concomitant economic rents in the billboards in ordinary space. But that hasn’t happened.
of interest related or unrelated to it. The actor will not stop following her, and will not stop talking to her.

Illustration 17A. Same as illustration 17, but the activity continues. The person reaches the building in which her office is located, takes the stairs to the 20th floor, and walks into her office. The actor follows her, continuing to babble on and on.

Illustration 17B. Same as illustration 17A, but the activity continues yet further. The person goes home but the actor follows her to her home, enters without her consent and continues to babble on and on.

Illustration 17 is not based on any particular case, and I leave it to those who specialize in such things to find the point at which the actor’s conduct passes from the level of annoyance to legally impermissible. If there is such a point, and it would seem that at least by the time of illustration 17B there is, then this illustration might provide some precedent against similar mischief in cyberspace. The result in ordinary space is not dependent upon the existence of any trademark, nor would it avail the actor to defend on the basis that the actor didn’t “use” any expression “as” a trademark. Likewise, the result in cyberspace is not so dependent. For my present purposes, however, the offense in cyberspace is limited to those arising out of the abuse of dynamic focal points to invade, deluge or ambush a user with uninvited or unwelcome material. Perhaps, as some including Professor Lessig have suggested, there is some sort of right to invade someone else’s privacy in ordinary space (or perhaps a duty to listen), but if there is some limit in ordinary space at the home or office door if not before, so there may be a limit in cyberspace at the gateway to the user’s access device. Indeed, because of the ubiquity and the ease of invasion, ambush, deceit and mischief, there is perhaps reason for more concern about privacy and freedom from invasive entries in cyberspace than elsewhere. The victim of unwanted attention can, at least close and lock a door in ordinary space and thereby seek and perhaps obtain some measure of self help, but such walls or barriers are sometimes much harder to maintain in cyberspace. Here is another example, this one from piberspace.

Illustration 18. A person left almost paralyzed by an automobile accident is able to speak with the assistance of a wireless brain-to-computer interface by which implanted electrodes within the person’s brain translate electrical signals into speech. An actor, just for fun, decides to see whether she can “hack” the code and, to prove the point, intercepts the signals, decodes them and then transmits related information into the person’s brain every time a focal point is detected. When confronted, the actor asserts that the conduct did not include any “use” of any expression “as” a trademark. In addition to whatever else may be involved, this conduct is at least a focal point offense by uninvited ambush and may, at the least, be subject to an “opt out” remedy by which a court would require the actor to obtain express permission from the person targeted.
This Article is, in a narrow sense, about focal points and trademarks in cyberspace. In that narrow sense, illustration 18 is beyond the scope. But more generally, I am proposing a comprehensive and coherent method for making sense of the code world and for designing a law for the code world. Illustration 18 is loosely based on advancing technology which may or may not develop in psiberspace, but which is certainly plausible.

One reason, among many, for resisting the notion that whatever problems we may see with focal point offenses in cyberspace, the solution must be found, if at all, within current notions of ordinary trademark law, is that the myopic concentration on trademark (and more generally, the obstinate refusal to design a law for the code world, but fecklessly and eagerly to contort ordinary law too rapidly without first seriously understanding the real relations at stake there) may lead to the law’s preemptive surrender of the ability to regulate the code world absent special statute or other contortions.

This illustration is given almost in jest, and in anticipation of further work to develop a law for psiberspace (I would expect the penalty in psiberspace would be much steeper than merely the required opt-out that suffices in cyberspace). I claim simply that existing common law, purposely transformed and designed for the code world, can already regulate such mischief without the need for any new statute, and regardless whether there is any trademark infringement involved. I haven’t time at the moment to develop the point any further than this—but if there is a binary choice in a case like illustration 18 between (a) no liability because no trademark infringement, and (b) liability by applying the proposed focal point analysis in a static manner from cyberspace to psiberspace, I’d opt for choice “(b)” even though I think we can do better than that by optimizing, refining and specifying the approach into one more suitable for psiberspace.

My general approach is to design law for the code world starting with the “nature and place” of the activity in question, and then proceeding to test whether the general nature and place of use factor can be rationally specified into a rule-specific form in the context of any particular place and any paradigmatic and recurring problem within that particular place in the code world. The focal point offense is a specified application of the nature and place of use in the context of cyberspace and within the further context of regulating focal points used as markers or spoilers, some of which incorporate trademarks. The focal point offense works with invisible and attenuated uses in cyberspace. I am not yet ready to publish a complete nature and place of use analysis as applied to other substantive

---


208 I have divided the code world, for ease of reference and relative to the designed purposes and problems of the various places within that world into: (a) the metaverse, (b) cipherspace, (c) psiberspace, (d) the blogosphere, and (e) cyberspace (or cyberspace proper). Because the real relations and recurring special problems are different in each place, it is well to treat each place separately when appropriate. The coming problems in psiberspace may be much more serious than those in cyberspace, but the practice of getting things more nearly right in cyberspace should have a high transfer value when it is time to address psiberspace. See the extended illustrations, from alpha to omega, for these more apocalyptic problems. Text at notes 175(alpha) - 181(omega) supra.
intellectual property or other problems involving new technological uses in the code world. Likewise, I am not yet ready to publish my extension of this analysis into psiberspace, cipherspace, or other domains within the code world. Nonetheless, I believe my general proposal for designing law for the code world is sufficiently robust to follow the new technological uses wherever they might lead, and is not limited by accidental forms and momentary standards of technology.

The following illustrations return to cyberspace proper, and to the problems of warehousing focal points, and of ambushing users of focal points:

Illustration 19. Same as illustration 8 (Ford.com), except the address is one that the actor obtains but chooses not to activate and so it effectively expropriates a logical focal point, preventing its use by another. The expression functions as a roadblock. This is an actionable cyberspace intervention (a focal point offense), the actor may continue the expropriating “use” (or “non-use”) but the actor’s conduct in obtaining and wasting the focal point may be such that a court would require the actor to provide a live “dummy” location reachable by the focal point and including in the dummy location at least a disclaimer and a redirect to the other.

Illustration 20. Same as illustration 19, but the focal point incorporates a trademark. Same result; and it is even more likely that the remedy will include at least the requirement that the actor create a dummy location with a redirect.

Illustration 21. Same as illustration 13, but the magnet is one that also effectively expropriates a logical focal point, in a way not preventing its use by others, but which adds “chaff” and false positives in cyberspace, making it more time-consuming to find or use the desired focal point as a navigational marker, and perhaps spoofing a spider, search engine or directory. That is, the actor arranges that the focal point triggers some other event in the code world which provides uninvited or false invitations. The expression of false invitations, and the expression of uninvited invitations each functions as a detour and/or as an ambush (compare illustration 17B). If this is an actionable cyberspace intervention (a focal point offense), the actor may continue the use but may be required to provide a reasonable technological accommodation including a disclaimer with a redirect on every “false positive.” At some level, a court may require an opt-out (or an opt-in) so that the actor may continue the conduct only with the consent of the person targeted.

Illustration 22. An actor places a magnet that includes an expression triggered by a person’s actions in cyberspace which are monitored by a

---

209 But cf. generally, Folsom, Non-Neutral Principles, supra note 18 (suggesting applications of the “polling” or sampling techniques to problems of secondary liability in cases involving new technological uses); Folsom, Embracing eBay, supra note 18 (suggesting applications of what is here denominated a “limited common remedy” to certain cases involving copyright and patent).

210 Compare illustration [3bis]. There the other (the mark proprietor) is able to use an active address, free riding as it were on the free-rider. Here, the other (the mark proprietor) is able to compel a use by the hoarding actor so as to exercise the advantage of its own focal point.
machine or virtual machine. The expression results in an intervention, including by ambush, directed to that person and which can be perceived, reproduced or communicated either directly by that person or with the aid of a machine or virtual machine, adding “chaff” or contextual advertising or other cyberspace traces. The expression may function as an ambush of the user. If this is an actionable cyberspace intervention (a focal point offense), the actor may be required to provide a reasonable technological accommodation including an order to cease use, or else permitted to continue use only upon provision (conspicuously provided to any recipient) of a clearly marked and easily accessible notice and “opt-in” coupled with (on a continuing basis) clearly marked and easily accessible notice and “opt-out.”

Illustrations 18-22 are based on cases that put pressure on ordinary principles of trademark-related law. Some cases have held, in essence, that a hoarder who takes trademarked expressions out of circulation causes a likelihood of confusion, or commits an act of forbidden cybersquatting, or violates a uniform domain name resolution procedure. The focal point offense reaches a much more rapid, uniform, predictable and measured result. Each of these expropriations or acts of spoilage is a focal point offense. Each is subject to the common remedy. The various interests are accommodated by rewriting the code. Important cyberspace navigation may continue, protected by the reasonable and effective technological accommodations.

2. Trademarks

Illustration 23. Same as in any of the preceding illustrations, but the offending cyberspace intervention involves use of a trademark which can be perceived, reproduced or communicated directly or indirectly including by way of a machine or virtual machine, and is used in connection with the marketing of goods or services even if the association is an attenuated one. If the cyberspace intervention (focal point offense) is also a trademark infringement, but only in the sense of an invisible, attenuated or expropriating use, the actor may be subject to any remedy appropriate under trademark law. The presumption is that the remedy should be selected from among the reasonable technological accommodations which comprise the common remedy for focal point and trademark-related offenses. In order to determine

---

211 See, e.g., PETA v. Doughney, 263 F.3d 359, 367-69 (4th Cir. 2001) (finding use, likelihood of confusion, and liability under the ACPA anti-cybersquatting provisions when a spoiler’s registration of a domain name contained the mark of another in an attempt to prevent a trademark owner from obtaining the domain name); Sporty’s Farm, L.L.C. v. Sportsman’s Mkt., Inc., 202 F.3d 489, 493 (2d Cir.), cert. denied, 530 U.S. 1262 (2000) (finding liability for cybersquatting under the ACPA, and for dilution under the FTDA when blocking a competitor by registering a domain name including the competitor’s mark and then assigning the domain name to a non-competing wholly-owned subsidiary; use was presupposed and no appeal was taken from the trial court’s rejection of trademark infringement claims because the parties were operating in wholly unrelated businesses); Panavision Int’l, L.P. v. Toeppen, 141 F.3d 1316, 1324-27 (9th Cir. 1998) (finding commercial use of the mark and liability for dilution under the FTDA when Mr. Toeppen obtained domain name registrations covering more than 100 well-known marks, including “Panavision” and “Panaflex,” and then set himself up in the “business” of selling them back to the trademark proprietors).
whether there is any likelihood of confusion, the new fully specified “nature and place of use” factor should be employed.

Illustration 23A. Same as illustrations 4, 4A or 4B, (the cyberspace offense occurs by use of a vanity phone number such as 1-800-HOLIDAY or a similar trapping expression) and it further appears that:

- the offending conduct is free-riding, intentional, calculated and unexpected (the caller expects to reach someone affiliated with Holiday Inns, but a person other than Holiday Inns has appropriated the focal point);
- the offending user is either a competitor of Holiday Inns or else a reservation broker who charges Holiday Inns for any referral of a customer to a Holiday Inn hotel;
- the “victim” is a caller who is simply trying to book a room at a Holiday Inn hotel;
- the place of use is the telephone side of cyberspace;
- there are findings on some ordinary likelihood of confusion factors: there is an intent to divert customers from Holiday Inns, there is a finding of actual confusion, there is a finding that the expression HOLIDAY is identical to the salient portion of a strong mark, and there is a finding that the goods or services are either identical or closely related; and
- there is preclusive-style initial interest confusion because there is a finding that the caller, once the call begins, is greeted by an active and aggressive salesperson who provides an ineffective notice of non-affiliation with Holiday Inns while at the same time affirmatively assuring the caller that there is no need to redial Holiday Inns because the salesperson can provide the same goods or services at the same price, and can also quote prices at comparable other lodging providers, thereby trying to prevent the caller from hanging up and dialing Holiday Inns and so depriving Holiday Inns of a chance to make the sale;
- the offending party has been asked by the mark proprietor to stop or else to provide a truly effective disclaimer (and to provide a forced redirect to a clean phone number), but has refused;
- the conduct constitutes at least one of the focal point offenses (here, it is at least a deceptive focal point which ambushes users); and
- there is no public interest in permitting the actor to continue to divert customers who are seeking Holiday Inns and who is, at the same time, unwilling voluntarily to provide an effective notice and forced redirect as a reasonable technological accommodation; and cyberspace navigation, and the interest in robust access and navigation is enhanced by prohibiting this offending use.

In addition to constituting a focal point offense (and in addition to the limited common remedy available for focal point offenses and for trademarks which are infringed only by an invisible or attenuated use), this conduct also constitutes trademark infringement by likelihood of confusion under the specified new “nature and place of use” analysis. As a result, the actor
becomes subject to the entire battery of trademark remedies and may be subject to an injunction prohibiting any further use of the expression in the actor’s vanity phone address, and the actor may be liable for damages.

Illustration 24. Same as illustration 23, but the use is visible to the user because it is advertised, promoted, and is directly associated with goods or services offered for sale. It is simply an example of “ordinary space” trademark infringement transposed to cyberspace, as would be the case of any expression placed on a page on the worldwide web visibly or audibly displayed as text, sounds, or audiovisual clips and used in association with goods or services, sponsorship or affiliation. The ordinary likelihood of confusion factors should be employed and the full set of trademark infringement remedies should be available.

Illustration 23 is the invisible or attenuated use which so troubles ordinary trademark law. It is already a focal point offense because it involves the use of a dynamic focal point (a marker) as address or magnet. Because the associative marker includes a trademark, it might also constitute a trademark infringement, but only if there is a likelihood of confusion. The new factor, the fully specified “nature and place of use” should now be employed to determine whether there is any likelihood of confusion. The common remedy, consisting of the appropriately matched reasonable technological accommodation, would apply.

Illustration 23A is a case in which there is both a focal point offense and also an independent trademark infringement, assessed according to the new fully specified “nature and place of use” factors for likelihood of confusion in respect of invisible or attenuated uses of trademarks in cyberspace. It is based on *Holiday Inns*, but it comes to the opposite result. There is a “use” because the conduct constitutes a deliberate appropriation and association of a focal point, either directly or indirectly by way of a machine or other device. It is a use which causes a likelihood of confusion because of the congruence of the factors. It is, as well, and perhaps ironically, a case that includes what might be called “true” or preclusion-style initial interest confusion. It is a “sticky” location in cyberspace. In combination with all of the other factors, this creates a finding of trademark infringement in cyberspace.

Illustration 24 is, finally, a case in which there would almost certainly be no need to do anything other than to apply “ordinary” principles of trademark law. If an electronic page on the worldwide web looks like, acts like, and functions like a page in an ordinary magazine, or if an audio sound recording functions like an ordinary radio broadcast, or if an audio-visual clip functions like an ordinary

---

212 According to the new likelihood of confusion factor: if the use is predatory, non-value adding and uninvited; if it is made by a spoofer or trapper; if it is directed at a user who is, in the context of the use, unaware or off-guard; if it is actually a preclusive-style of initial interest confusion; if it occurs in the invisible and attenuated realm of “high” cyberspace where augmented presences are particularly vulnerable; if the actor has failed to respond to “polling” which might have defused any confusion; if there are other relevant factors from ordinary trademark likelihood of confusion which tend towards a rational assessment of likelihood of confusion; if there is tampering, spoofing, ambushing or spoiling, then there may be a finding of trademark infringement. See section I., supra (discussing the new factor).

213 *Holiday Inns*, Inc. v. 800 Reservation, Inc., 86 F.3d 619 (6th Cir. 1996).
television show or motion picture, then (finally) we might expect to be able to apply ordinary principles of trademark law. Ordinary trademark law can cover trademark-related offenses in cyberspace, but only if, and only to the extent the offenses in cyberspace merely recapitulate offenses from ordinary space. The problem is that the paradigmatic conflicts in cyberspace, illustrations 2-23, are precisely those focal points encompassing invisible and attenuated uses of markers or spoilers functioning as address, magnet, roadblock or detour, and which do not recapitulate ordinary space. Where there is a simple case of transposition, as in illustration 24, we simply transpose ordinary principles including prophylactic remedies.214

The comparison between illustrations 23 and 24 illustrates the differences, similarities, overlap and distinction between the focal point offenses, the cases of trademark infringement by likelihood of confusion arising out of invisible or attenuated uses in cyberspace, and those instances of likelihood of confusion that are visible and direct. If we are speaking only of an ordinary conflict merely transposed to cyberspace, visibly and directly, then it follows that ordinary principles of trademark law actually do apply (illustration 24). But if we are speaking of the characteristic mark-related conflict in cyberspace which involves invisible and attenuated uses of marks incorporated within dynamic focal points, then ordinary principles of trademark law are not well suited, and a new factor must be employed (illustration 23A).215

3. Resource Providers (Secondary Liability: targets and safe harbor)

Illustration 25. Same as in any of the preceding illustrations, but there is another person who might be secondarily liable because of fault (contributory or inducement-style of secondary liability), status (the agency or the “expanded for copyright” version of respondeat superior-style), consent (suretyship-style secondary liability), or policy, and the other person has offered to provide a reasonable technological accommodation, with costs to be shared by the claimant. If the underlying conduct is an actionable cyberspace intervention (a focal point offense), then the underlying cyberspace intervention may be subject to the appropriate cyberspace remedy, and the other person, if secondarily liable, may be required to provide a reasonable technological accommodation and the claimant may be required to share the costs. See illustrations 14-16.

214 That is to say, if, for example, it were the case that a web site included a page displaying an ordinary infringing use of a trademark as assessed under an ordinary test for likelihood of confusion and an injunction against such use was warranted, then it might well be appropriate to enter an injunction against coincident invisible and attenuated uses, and so bar the use of the offending expression in an address or as a magnet. The explanation would be that those coincident uses, otherwise subject only to reasonable technological accommodations, might now be barred to help undo the harm of the ordinary trademark infringement. Cf. Brookfield Commc’ns, Inc. v. W. Coast Entm’t Corp., 174 F.3d 1036 (9th Cir. 1999) (barring some such coincident uses without any showing of any ordinary infringement on the web page itself).

215 I claim that ordinary principles not only have led to the problems of over- and under-protection, but also that even when the extremes are eliminated and expressions are simply evaluated on the correct understanding that some (but not all) of them might cause a likelihood of confusion, the currently existing ordinary principles of likelihood of confusion are simply inapt. See infra text at notes 236-256 (asserting that the ordinary factors lead to false positives or to weak or null inferences in cyberspace).
One of the more substantial risks of current trademark infringement analysis when applied to invisible and attenuated uses in cyberspace is that there is a reciprocal relationship between direct liability and secondary liability as applied to new technological uses. This creates a double pressure, tending towards bad results in both directions. On the one hand, there is a healthy concern not to apply ordinary principles of trademark law so as to find direct liability for infringement, for fear of creating potentially crippling secondary liability on value-adding resource providers to the detriment of new technological uses. On the other hand, there is the consequence that, where there is no direct liability then there grows a sort of “anything goes” regime which would disfigure cyberspace by making it an outlaw zone in which tampering, spoofing, ambushing, waste and spoilage ruin its promise of access, navigation, information-activity, and trustworthy augmented presences. This might lead to a pressure to find some sort of secondary liability, especially where the direct actors are hard to find, hard to serve, and hard to remove (and the secondary liability actor is an easy target). The focal point offense analysis and the new “nature and place of use” factor for assessing likelihood of confusion for invisible and attenuated uses in cyberspace, coupled with the limited common remedy, solves this problem.

B. Cases

The most significant of the mark-related cases in cyberspace are those involving invisible, attenuated or expropriating markers or spoilers and those in which current judicial decisions have not focused on the offending use of the marker or spoiler as a deceptive focal point, but have attempted to apply a trademark analysis. In so doing they have: (a) threatened the ability of a value-added mapper or guide to produce an index to cyberspace (a directory or search engine, functioning as a “hitchhiker’s guide” for the benefit of surfers in cyberspace) or to sell keyword triggered advertising to pay for it, (b) impaired the ability of a user freely and reliably to access and navigate within cyberspace, (c) threatened the ability of a value-added mapper or guide to produce an index to cyberspace (a directory or search engine, functioning as a “hitchhiker’s guide” for the benefit of surfers in cyberspace) or to sell keyword triggered advertising to pay for it, and (d) threatened the ability of a user freely and reliably to access and navigate within cyberspace.

---

216 Folsom, Non-Neutral Principles, supra note 18.
217 The threat is both of direct liability and of secondary liability. The potential for expanded secondary liability is not negligible and the reported cases continue to probe the boundaries. Playboy Enters. v. Netscape Commc’ns Corp., 354 F.3d 1020 (9th Cir. 2004) (copyright case: suggesting broad a potential for broad secondary liability in cyberspace); Perfect 10, Inc. v. Visa Int’l Serv. Ass’n, 494 F.3d 788 (9th Cir. 2007) (copyright case in cyberspace: rebuffing, over a strong dissenting opinion, secondary liability asserted against a credit card issuer claimed to have been put “on notice” of the asserted infringing activities for which the credit card issuer was providing otherwise ordinary payment system settlement services); Tiffany, Inc. v. eBay, Inc., 576 F. Supp. 2d 463 (S.D.N.Y. 2008) (trademark case in cyberspace: involving a claim that an online auction provider, though taking steps to police counterfeit marks used by third party sellers, had yet not taken steps sufficient to defeat secondary liability) (the online auction provider prevailed). Although the cases struggle to prevent the imposition of unbearable secondary liability in cyberspace, the potential for such liability is real because the legal rules of secondary liability as developed in “ordinary” space certainly might literally apply to conduct in cyberspace which is, because of the power of code, within the capacity of a third party to “know” or to “have reason to know” or to “control” or to “have the power to control” and so on. See Non-Neutral Principles, supra note 18, text at n. 172.
218 The threat is not only of deprivation of navigational markers but also of the superabundance of them. Compare, e.g., Brookfield Commc’ns, Inc. v. W. Coast Entm’t Corp., 174 F.3d 1036 (9th Cir. 1999) (depriving), with Holiday Inns, Inc. v. 800 Reservation, Inc., 86 F.3d 619 (6th Cir. 1996) (superabounding) and 1-800 Contacts, Inc. v. WhenU.Com, Inc., 414 F.3d 400 (2d Cir. 2005) (superabounding).
(c) harmed the characteristic values of cyberspace, or (d) sown confusion and discord, by doctrinal creep, reverse doctrinal creep or equivocation, into the “ordinary” law of trademark, unfair competition and cognate legal fields. These cases are particularly difficult for current law to get right.

Representative current cases tend towards opposite errors of over-protecting marks in space upon a radical misapplication of initial interest confusion, or under-protecting marks in space by conjuring an independent use-as-a-mark requirement.

The harms of overprotection are many and clear. Overprotection denudes the virtual map to cyberspace by depriving surfers of focal points they want to use in a nominative sense to find locations, persons, places and communities of interest. It hampers the providers of virtual maps by reducing prime revenue sources relating to focal points by depriving them of some of the higher value keywords for sale as markers. It flattens trademarks by wrongly treating essentially unknown expressions as if they were distinctive enough to result in automatic infringement. It generally spoils cyberspace by imposing more control than is necessary or good for it.

In passing, it should not be overlooked that overprotection of marks in cyberspace also contributes to the general over-expansion of trademark in ordinary space.

The harms of under-protection may not be quite so clear, but they are every bit as real. Under-protection creates a juridical abdication, leading to an outlaw zone in which measures (fences) and counter-measures (fence-cutters) are left to fight it out. The resulting chaff obscures and overwhells the virtual map of cyberspace by deluging it with false positives (markers that lead nowhere or off-subject), effectively denies access and navigation by covering the reliable markers with so many false leads as to frustrate the surfer, takes advantage of augmented presences by leading them to places they had no intention to visit, and destroys trust. The chaff also constitutes invasive monitoring of and intrusion into the surfer’s real or imagined intention and volition, and it interferes with and diminishes the business of the directory and search engine providers by thwarting their efforts to produce the “global phone book” or “hitchhiker’s guide” that makes cyberspace possible.

The cases do not purposefully distinguish space pirates from value adding mappers and guides. Instead, the tendency of the currently conflicting approaches is to exonerate the pirate who does not “use” its marker or spoiler “as” a mark, while at the same time threatening the legitimate user, and the value-adding resource provider, who somehow directly causes, or indirectly incurs secondary liability arising out of some initial interest confusion by way of an invisible or

---

219 Any action that denies access, impedes navigation, impairs information-activity, takes advantage of augmented presences, or destroys trust harms the characteristic values of cyberspace. These, and other values, may be discerned in other places within the code world.

220 Folsom, Space Pirates, supra note 17 at 864-69.

221 Id. at 845-48; and see e.g., Brookfield, 174 F.3d 1036; Netscape, 354 F.3d 1020.

222 Folsom, Space Pirates, supra note 17 at 848-50.

223 Id.

224 Holiday Inns, Inc. v. 800 Reservation, Inc., 86 F.3d 619 (6th Cir. 1996); 1-800 Contacts, Inc. v. WhenU.Com, Inc., 414 F.3d 400 (2d Cir. 2005); but see Rescuecom Corp. v. Google Inc., 562 F.3d 123, 127-31 (2d Cir. 2009) and other cases cited, supra notes 62 & 63 (distinguishing 800-Contacts and perhaps signaling the end of the “no use” doctrine).
attenuated address or magnet. The distinctive mark-type disputes in cyberspace are difficult for current law to handle. Ordinary trademark law depends upon likelihood of confusion, and upon a fixed, relatively homogeneous or at least moderately static set of ordinary consumers against which to assess likelihood of confusion. It is ill-equipped to deal with multiple and sequentially changing contexts of invisible, attenuated and expropriating markers and spoilers in space.

In sharp contrast to current law, which provides no language to describe the concepts, my proposed new terms: address or magnet (markers), roadblock or detour (spoilers) as types of invisible, attenuated and expropriating uses—focal point offenses—serves to reframe the issues. The defined cyberspace offense names the nature of the harm. The distinction between pirate and guide helps to fix the normative target. The carefully limited remedy will ensure that the cure, a reasonable technological accommodation making a minimal demand on cyberspace actors, is not worse than the disease and actually cures the illness without killing the patient.

Even though invisible, attenuated and expropriating uses cause an objective effect, current approaches fail carefully to distinguish among those effects. They offer no way to sort out reliably the harmful cyberspace intervention from the beneficial or harmless. Even though using designations in space as address, magnet, detour or roadblock sometimes causes manifest confusion of source, sponsorship or affiliation in marketing the actor’s goods or services, or prevents another from using its own mark, current approaches fail to distinguish spoofers, pirates and shills from legitimate map-makers, guides and advertisers. The difficulty of assessing attenuated likelihood of confusion under current approaches is multiplied by the dramatically different, occasionally opposed and sometimes shifting strategies and factional interests of the characteristic users (and potential victims) in cyberspace.

In fact, the law is not getting the cases right, but is on a path that will either cripple cyberspace or disfigure the law itself. The leading representative cases are not only wrong, but also jeopardize the characteristic values of, and the public interest in, a robust and freely navigable cyberspace. The characteristic values of an objective cyberspace include access, navigation, information-seeking activity, augmentation and trust. The desired remedy for mark-related attenuated or invisible uses in cyberspace ought not to disserve the public interest. Instead it should, if possible, demand nothing more (nor anything less) than a reasonable technological accommodation in the public interest.

Here is how the focal point analysis answers some of the major (the “classic”) questions involving mark-related offenses in cyberspace, as put by typical
commentators, and as summarized in a prior Article:

(1) Is it trademark infringement to embed another’s trademark in an Internet domain name? Or in a phone number? What if the offending expression is merely warehoused by a domain name or phone number registration unaccompanied by active use of the offending Web site or phone number? What if the offending party does not initiate any sale of the expression back to the proprietor or otherwise avoids the indicia of the clumsy cybersquatter? And what if the expression is a mark not famous enough to qualify for anti-dilution protection?

(2) Is it trademark infringement to embed another’s trademark in HTML metatags or in buried code, tags, or invisible (hidden) text?

(3) Is it trademark infringement to sell advertising triggered by a trademarked expression? Does it make a difference how the trigger is set or activated, how it is marketed or bundled, or whether it is associated with a disclaimer of some sort?

(4) Is it trademark infringement to sell enhanced relevancy rankings? And is it trademark infringement to spoof a relevancy ranking system by a method relying in part upon some use of a trademarked term?

(5) Is it trademark infringement to embed another person’s trademark as part of an e-mail address or as a subdirectory name?

(6) Is it trademark infringement to associate another’s trademark with spam messages or fraudulent, illegal, or other unwelcome intrusions?

(7) Is a disclaimer enough to avoid liability in any or all of the situations in which there might otherwise be liability for an invisible or attenuated use? Can the law require a disclaimer, or can the law require any other reasonable steps to avoid “passing off” or likelihood of confusion? Does bad faith figure? Does actual confusion? Does “direct” versus “indirect” (vicarious or other grounds for secondary liability) afford a meaningful basis for distinguishing and providing different legal responses to, say, the person who purchases a trademark-triggered keyword and associates it with an advertisement for goods or services, as opposed to a resource provider who merely sells or otherwise enables the trademark trigger that is then employed by another person as an invisible, attenuated, or expropriating marker or spoiler in space?\(^2\)

The first observation is that the questions are not well put and so cannot be

\(^2\) Space Pirates, supra note 17 at 854-55 (stating that the answers to these questions would have to await a further Article, and anticipating that this current Article would revert to those questions). It should be no objection that the answer, implicit there, is not particularly complex but required more space than was available there.
well answered. A better question would have been: could any of these activities constitute conduct in connection with marketing goods or services which might possibly constitute trademark infringement if they cause a likelihood of confusion? The answer, almost painfully simple, is this: “yes” all of these (except perhaps the embedding as an internal subdirectory name, per (5) above) could do so. This is, to be sure, just another way of asking the “use” question.

Another, and even better way to put the question would have been: do any of these activities constitute focal point offenses? The answer, almost as embarrassingly simple is: “yes” most of them, except the internal subdirectory name, probably do. Whether any one of them actually does or not will depend upon whether, in the circumstances, the particular conduct constitutes tampering, spoofing, ambushing, or spoiling. But where there is a focal point offense, then the legal consequence is merely to invoke the common remedy to require a reasonable technological accommodation, no more and no less.

One might almost wish the answer were more difficult, esoteric, cunning or strange. But it isn’t. The focal point offense is, and is intended to be, a heuristic rule of thumb to dispose of cases efficiently. It routinely reaches the correct result, for the right reason, persuasively explained. Nothing more is required. Of course, some or all of these might also constitute an instance of trademark infringement. Whether they do or not would depend even more heavily upon the particular circumstances, and the new fully specified “nature and place of use” factor for likelihood of confusion identifies the relevant evidence for assessing trademark infringement. At the conclusion of any trademark infringement analysis, however, we would apply the same common remedy as would be applied under the focal point analysis. Since the focal point analysis is so much more efficient and anticipates the same common remedy, I claim we may leave the trademark infringement questions to be resolved if and when they arise, and then based upon a full factual record developed on actual evidence in accord with the new factor for assessing likelihood of confusion.

The focal point analysis disposes at once of those prior exemplar cases that represented over-protection, and the opposite extreme that represented under-protection. It resolves the paradox of those two lines of cases, and likewise disposes of those so-called middling cases that existed perhaps uneasily between the two extremes. Finally, it saves us from the inapt factor analysis that was devalue that which is too easily gained, as Juliet warns Romeo that if he think her “too quickly won” and her behavior “too light” she will nonetheless prove “more true than those that have more cunning to be strange”).

A “high quality” opinion is one that “reaches the correct result for the right reasons in a manner that is persuasive and well-written.” 20 Questions for Howard Bashman, ACAD., May 6, 2003, http://theacademy.blogspot.com/2003_05_04_theacademy_archive.html#93864929 (emphasis added).

[227] Cf. WILLIAM SHAKESPEARE, ROMEO AND JULIET, Act II, scene ii, ll. 95-100 (suggesting a tendency to value that which is too easily gained, as Juliet warns Romeo that if he think her “too quickly won” and her behavior “too light” she will nonetheless prove “more true than those that have more cunning to be strange”).

229 A “high quality” opinion is one that “reaches the correct result for the right reasons in a manner that is persuasive and well-written.” 20 Questions for Howard Bashman, ACAD., May 6, 2003, http://theacademy.blogspot.com/2003_05_04_theacademy_archive.html#93864929 (emphasis added).

230 Space Pirates, supra note 17 at 845-48.

231 Space Pirates, supra note 17 at 848-50.

232 Space Pirates, supra note 17 at 850-52.

233 In cyberspace, the factor analysis breaks down. Strength of mark is leveled because to a search engine, an expression is an expression; overall commercial impression is out the window, because an invisible or attenuated use makes no impression; the “sophistication” of the consumer is meaningless because these are shifting, changing, impossible to predict audiences of surfers, shoppers, searchers, consumers of varying levels of interest and sophistication and even the most able might still be ambushed; and so on and so on. See [cite Polaroid, DuPont, and however many factor-list cases as make the point]. Because the ordinary cases ask
waiting around the corner in trademark infringement cases once it was determined that not every case must necessarily lead to initial interest style liability, and that most cases do constitute at least the kind of use which requires an assessment whether it is a causes a likelihood of confusion.

The trademark likelihood of confusion factors simply do not work because they are inapt to judge cases of invisible and attenuated uses. Consider the Polaroid, and related factors.

1. Strength of mark: this factor is leveled in cyberspace because all dynamic focal points are very nearly equal in the eyes of the search engines which process them. The non-human machine that registers expressions makes no necessary distinction between the focal points that incorporate very weak ("contacts"), moderately weak ("moviebuff"), and strong ("playboy") trademarks. The expression incorporating a trademark either is, or is not, a focal point. This leveling leads to false positives because every focal point simply is a focal point and each may be equal in the "eyes" of the search engine. It ignores the reality of legitimate cyberspace navigation by way of nominative focal points.

2. Degree of similarity between expressions: this factor is leveled because all focal points are magnets or spoilers; all legitimate markers incorporating a trademark are intended to point to the inherent or associated person, place or community of interest; and this will only happen if the expression incorporating a trademark is identical or very nearly identical to the mark at issue. This factor would lead to false positives, because it will embrace the totality of the universe of focal points that incorporate a trademark and will eliminate none of them. If this factor, or some combination of it and the third factor (product proximity) really are the lead or driving forces in providing a dispositive negative finding–no likelihood of confusion—then the inherent

questions that are at best irrelevant to invisible and attenuated uses in cyberspace they will return useless answers.

I have commented on this view, and collected a sampling of the authorities, supra, at notes 46-53. Notwithstanding the arguments of some, it certainly seems the "no use" doctrine is outside of mainstream trademark law, and is of no use in regulating mark-related conflicts in cyberspace. I have defended this view, and collected a sampling of the authorities including at least some who disagree with my conclusion, supra, at notes 54-72. See Space Pirates, supra note 17 at 864-69 and passim (claiming both that the "use as" requirement is an innovation and that it is an unnecessary innovation because cyberspace interventions can and should be resolved on the merits and without the necessity of an awkward "use as" gatekeeper).


Polaroid, 287 F.2d at 495; see RESTATEMENT §21(d) & cmt. i (discussing the distinctiveness or "strength" of marks).

This expression was at issue in 1-800 Contacts, Inc. v. WhenU.com, Inc., 414 F.3d 400 (2d Cir. 2005). The court avoided the issue by holding that there was simply no "use" and so did not analyze strength of the mark (or any other likelihood of confusion factor).

This expression was at issue in Brookfield Commc’ns, Inc. v. W. Coast Entm’t Corp., 174 F.3d 1036 (9th Cir. 1999). The court avoided grappling with the issue by holding that there was initial interest confusion.

This expression was at issue in Playboy Enters. v. Netscape Commc’ns Corp., 354 F.3d 1020 (9th Cir. 2004). The court avoided grappling with the issue by holding, in the preliminary posture of the case, that the plaintiff may have properly alleged initial interest confusion. It would seem "playboy" is no stronger or weaker than "contacts" when it comes to attracting a search engine.

Polaroid, 287 F.2d at 495; see RESTATEMENT §21(a) & cmts. c, d, e, & f (discussing the comparison of designations).

See Barton Beebe, An Empirical Study of the Multifactor Tests for Trademark Infringement, 95 CAL. L.REV. 1581 (2006) (drawing upon data for a 5-year period, and concluding the data show that non-similarity is a
hobbling and nullification of these factors necessarily ham-strings any such “knock-out” heuristic.

3. Proximity of products: this factor is irrelevant to the focal point problem because regardless whether the products are the same or related or wholly unrelated the expression remains a focal point in cyberspace and persistently draws traffic, blocks traffic, or ambushes or ensnares a user. This leads to misplaced or weak inferences. The positive inference from products that are the same or related is in the nature of commercial marker problems: expressions that draw traffic to a competitor. The positive inference from products that are wholly unrelated is in the nature of spoiler problems, expressions that block, hinder or detour. Because commercial markers do not exhaust the category of focal point abuses, but leave the cases of non-commercial markers, and all spoilers untouched, the simple negative inference from a non-competing marker is not dispositive. Moreover, there is no necessary inference that a person using a focal point as a commercial (or non-commercial) marker to draw traffic to a person, place or community of interest is doing anything other than aiding navigation by providing nominative clues and without improperly trading on anyone’s goodwill.

4. Likelihood the proprietor will bridge the gap: this factor is equivocal at best. A first sense of the “gap” factor is to test product-proximity (for the stated purpose of the Polaroid test—it is meant to gauge the likelihood of confusion for unrelated products). But a second sense of the “gap” factor, as it might be applied in cyberspace is the perhaps odd notion that there is some sort of media gap apart from any product gap. It is as if we are seriously concerned whether the proprietor will bridge the gap from selling in the “brick and steel” of ordinary space into some world of “cyberspace.” In flirting with this second sense of the concept, it must be that we are either asking this question as if it were a matter of geographic priority (as if ordinary space were like Kansas, and cyberspace were like Nebraska) or as if it were a question of media (as if ordinary space were like radio, newspaper or billboard, and cyberspace were like television or posters on the sides of busses). No matter how the question is put, it is hard to see how it is either relevant or helpful. To suppose there is some meaningful gap between the brick and steel, and the virtual store is to introduce the anomaly of media-centric divisions, or to fly in

dispositive factor).

243 Polaroid, 287 F.2d at 495; see RESTATEMENT §21 (e), cmt. j (discussing the competitive proximity of the products).

244 They might be related as competitive, substitutional or complementary. They might be used by a “consumer” in a comparative or nominative sense. They might be used to find a community of interest or disinterest in the goods or services associated with the dynamic focal point.

245 A dynamic focal point coupled to an unrelated product might still trap, capture, disrupt or spoil navigation tied to the intended focal point.

246 Beebe, supra note 242 (concluding that in ordinary space, the data show non-proximity is dispositive against a finding of likelihood of confusion).

247 Polaroid, 287 F.2d at 495; but cf. RESTATEMENT §21, cmt. a (stating that “bridging the gap” is “not relevant to whether prospective purchasers are likely to be confused, but rather to the likely consequences of confusion, and hence to the nature of the relief that is appropriate if confusion is likely.”).

248 If there is a geographic priority question it should be asked directly rather than under the rubric of “gap bridging”, and if there is a question of marketing or advertising channels it, too, should be asked directly. Both questions seem odd in the context of cyberspace.
the face of the “good faith” standard for the second user in virtual geographic divisions.

5. Actual confusion: this is a factor that is certainly applicable, but not very helpful. It suffers from all of the same inference-confidence problems as in ordinary space, but it also suffers from the cyber problem. That is, the likelihood of confusion must be among an appreciable number of ordinary consumers. And then the problem is redoubled by the shifting, sequential, and vulnerable roles any user might from time to time inhabit. In contrast, the advantage of the new factor is that, by taking advantage of the coded reality of cyberspace it is possible to poll the “victim” at the point of the intervention, thereby reliably to measure the user’s actual status in real time and without any need for hindsight reconstruction or statistical modeling of what “might have happened.”

6. Intent (reciprocal of the defendant’s good faith in adopting the offending expression): this is a factor that will produce predictable false positives because most persons who design focal points intend to draw traffic, or to spoil another’s use. One might presume that a good many of them do so in “good faith” or might arguably claim they do not intend to infringe a trademark by doing so, but the point of the common remedy is to ensure that the focal offense is remediated by a reasonable technological accommodation. The very nature of the accommodation, or a refusal to accommodate, should serve as a proxy for good faith or bad faith and it would be a more meaningful indicator. In this respect, there is a good match between the predictive value of “bad faith” in ordinary space and the deliberate refusal voluntarily to provide reasonable technological accommodations in cyberspace. The advantage to the new factor is the ability reliably to test by the technique of sampling or polling at the point of the contested action.

7. Quality of the defendant’s product: this is an idiosyncratic, if not erroneous factor in ordinary space and is no more conclusive in cyberspace. This is, at best, a leveled factor in cyberspace.

8. Sophistication of the buyers: this is not helpful in assessing the problem in cyberspace because spoofing or ambushing, spoilage or waste may very well have their effect regardless of sophistication. The potentially

249 Polaroid, 287 F.2d at 495; RESTATEMENT §23.
250 Actual confusion is, so it is said, capable of proof in ordinary space by well-designed survey evidence. But at least one empirical study supports the conclusion that “surveys are rarely presented by parties or credited by courts.” Beebe, supra note 242.
251 The contrast between my proposed new/transformed factors and old factors helps to illuminate the difficulties of the old factors. The new factor is set forth supra in the text at notes 149-159.
252 Polaroid, 287 F.2d at 495; RESTATEMENT §22.
253 Beebe, supra note 242 (concluding “bad faith” is, in fact, dispositive of likelihood of confusion).
254 As in the case of the prior factor, I am getting ahead of myself here, but the contrast between new and old factors helps to illuminate the difficulties of the old factor. The new factor is set forth supra in the text at notes 149-159.
255 Polaroid, 287 F.2d at 495; see RESTATEMENT §21(e) & cmt. k (discussing how markedly different quality may suggest different purchasers or different market channels, or otherwise unlikely to be associated with a common source, and how evidence of inferior quality “is more properly relevant to fashioning appropriate relief if a likelihood of confusion is otherwise established.”).
256 Polaroid, 287 F.2d at 495; see generally RESTATEMENT §21(c) & cmt. h (discussing the “care exercised by” purchasers in combination with their buying habits as constituting factors that “can be important.”).
sophisticated or careful buyer, if ambushed, is as vulnerable as the 
unsophisticated or careless. In addition, many cyberspace visitors shift and 
change roles within a single session in space and might be sometimes 
sophisticated and “on guard” and sometimes not. As a result of the intrinsic 
heterogeneity of cyberspace users there is no unitary “hypothetically 
reasonable” buyer. Accordingly, this is a factor with limited inference 
confidence.

In comparison with any attempt to assess likelihood of confusion under 
ordinary factors that are not helpful, the focal point offense directly focuses on the 
real and underlying potential offense—tampering, spoofing, ambushing, trapping 
and spoiling. Beyond this, the new factor permits rational assessment of trademark 
infringement for the residual cases in which that inquiry must be faced. Does a 
focal point that incorporates a trademark constitute a “use” for potential trademark 
infringement in cyberspace?\textsuperscript{257} Does it cause a likelihood of confusion in 
cyberspace?\textsuperscript{258} In further comparison, the new nature and place of use factor for 
likelihood of confusion in cyberspace actually distinguishes pirates from guides, 
and divides predatory and harmful practices that cause a likelihood of confusion 
from the beneficial or neutral practices or effects of resource providers, guides and 
markers that do not cause any harm or likely confusion. And both the focal point 
offense and the new factors for likelihood of confusion let the remedy fit the 
offense by fixing the problem of the poisoned flower in a Pareto superior move.

C. Avoiding Spectacular Error

The current, wrong-headed approach might simply result in a series of 
accidental, non-systemic and perverse adjudications, merely adding a random 
element to the cost of doing business.\textsuperscript{259} If that were all, actors might simply learn 
to treat the occasional juridical lightning strike, hundred year flood, or earthquake 
as some sort of “act of God” and as a matter of rational indifference, merely ignore 
what cannot be rationally controlled. But the systemic nature of the problem 
suggests it will not be so easily cabined.\textsuperscript{260} Improperly applied, trademark law with 
its broad prohibitory injunctions in cyberspace can certainly kill the use of the 
most obvious and valuable navigational focal points, notwithstanding many users 
are far from experiencing any likelihood of confusion but simply because some 
plurality of users might be dazed, delayed or otherwise inconvenienced. At the

\textsuperscript{257} Yes, if it is conduct which includes any use of an expression in a manner that may be perceived, 
reproduced or communicated, directly or indirectly by way of a machine or other device now known or hereafter 
developed, even if not ordinarily perceptible by a person or only remotely associated with goods or services. See 
supra, text at note 150.

\textsuperscript{258} It depends. The new likelihood of confusion factor assesses the nature of the conduct, the nature of the 
offending actors and the nature of their victims; the place of use relative to the degree that cyberspace values are 
implicated; the presence of any other relevant trademark-related factor; the presence of real time polling, or of 
tampering, spoofing, ambushing, or spoiling; and the public interest in a robust and freely navigable cyberspace. 
See supra notes 151 to 159 (glossing the new factor).

\textsuperscript{259} Folsom, Space Pirates, supra note 17 at, e.g., 889 (observing that many of the most striking and oft-
cited representative cases are not only wrong, but exactly wrong, often exonerating the predator or free-riding 
opportunists while putting the value adding resource provider in the cross-hairs of potential liability).

\textsuperscript{260} Folsom, Missing the Mark, supra note 16 at 228-34 (applying Professor Bainbridge’s analysis of 
systemic juridical risk to cases involving mark-related conflicts in cyberspace).
same time, and if trademark law is improperly applied from the other direction, open and unchecked uses of trademarks (and other focal points) can lead to such a barraged, deluged, spoofed and deceptive environment that a user’s field of navigation might shrink to such a narrow zone of cyberspace as to abandon the promise of active-information altogether.

The new approach not only more nearly gets to the correct result, for the right reason, persuasively explained than does any of the existing approaches, it also avoids the specter of spectacular error. Because of the common remedy, the worst that can happen from a clumsy or mistaken adjudication is a reasonable technological accommodation. Life in space goes on, the robustness of cyberspace is preserved, all the interests are accommodated, and at reasonable cost.

III. COUNTING THE COSTS OF THE NEW FACTOR: IT IS EFFICIENT

The focal point offense and the new likelihood of confusion factor are affordable. New institutional economics seems to constitute a better model than a micro-economics model for projecting costs and benefits for trademark-related law in cyberspace. This is, in part, because the phenomena of a feedback loop and doctrinal creep in trademark generally, and exacerbated in cyberspace specifically by the shifting factional interests involved, seems to make micro-economics an exercise in non-empirical and non-verifiable guesswork at this point due to an apparent lack of reliable data from which to calculate micro-economic costs.

When it comes to counting the costs, there are three constituencies or groups: (1) the primary users of cyberspace who cause or suffer the consequences of focal point and mark-type disputes; (2) the juridical actors who must negotiate, structure, resolve, regulate, teach or explain the results; and (3) the public whose perception of the rule of law is itself something worth considering.

The key point is that, based on the nature of cyberspace itself and the reasonable technological remedy inherent in the new analysis, the new factor not only simplifies legal regulation, but it naturally readjusts the economic and normative influences under the modest regulatory power of a law designed for cyberspace. The power is in the forced redirect and reciprocal auction. I predict these remedies will eventually drive the price of focal point abuse down toward its cost, remove and reverse the effects of economic rents currently incentivizing focal point abuse, and restore to cyberspace navigation the non-scarcity-driven-economic paradigm of objects created by code. This economic tendency complements a deliberately selected set of norms in cyberspace. The focal point offense and related economic model select the open access and open navigation norm, and they reject the piratical or predatory norm of cyberspace. As a result, all persons, places, and communities of interest that can exist in an open-access, freely navigable code world, will. The intrinsic economics of the limited common remedy for focal point offenses cause the proposed solution to be Pareto-optimal for all users except the pirate, predator, parasite, vandal, and spoiler.261 At the same

261 I (and Professor Lessig) have claimed, at the outset, that recoding Martha’s poisoned flowers so they won’t kill Dank’s next dog is a Pareto-optimal result. I suppose that if Martha actually enjoyed killing dogs, and if she actually were committed to predatory values, then the solution would no longer be optimal from her perspective. But I don’t care. I have urged, and continue to urge that the law should take sides on questions of first principle that also have economic or other manifestly consequential effects on others, and that it deliberately
time, the simplicity of the focal point offense—inquiring whether the challenged
conduct tampers, deceives, ambushes, or spoils cyberspace—makes the new
approach efficient to administer, explain, and to anticipate. This, in turn, makes it
easier and more efficient to invest in new technology, and to plan for new
technological uses involving focal points in space. The reader who already sees
these connections may skip to Section IV, but might still find it profitable to
browse this Section to confirm the relationships already suggested.

The following sections divide the persons affected into separate factions or
classes since each class has its own mix of anticipated benefits and burdens
deriving from the proposed new factor, but then evaluates them according to the
common good of cyberspace. Cyberspace is characterized by a plurality interests
and further marked by the fact that a single user often shifts sequentially from one
mode to another, and might simultaneously act in multiple capacities or interests.
This makes generalized statements about “ordinary cyberspace users” almost
meaningless and it frustrates all of the current attempts to gauge or guess
likelihood of confusion in space which fail to distinguish shifting factional
interests from a public interest. The classifications used in this article aim to cut
across the changeable nature of the individual users and to provide some more
nearly fixed reference points for meaningful and purposeful general analysis. It is
intended to bring into focus the public interest in a robust and freely navigable
cyberspace as against the parochial interest of any faction of users who happen to
be there.

Part A of this Section will deal with the primary users who cause or suffer the
consequences of focal point offenses. Cyberspace users include the invited or
uninvited, value-adding or free riding, harmless or predatory surfers and mappers,
spoofers and trappers, spoilers and arbitrageurs, shills and advertisers, shoppers
and consumers, competitors and mark proprietors who cause or who suffer from
mark-type conflicts in cyberspace. Among the actors are some who are, in fact,
pirates and plagiarists. The “pirate” in cyberspace is anyone committing a focal
point offense.

Pirates and plagiarists are defined terms in my work. Supra note 133. I do not use them loosely as
some have done, but as specified words. Compare Graver Tank & Mfg. Co. v. Linde Air Prods. Co., 339 U.S.
605, 612-13 (1950) (Black, J., dissenting) (objecting to a very loose usage of the word “pirate”: “I heartily agree
with the Court that ‘fraud’ is bad, ‘piracy’ is evil, and ‘stealing’ is reprehensible. But in this case, where
petitioners are not charged with any such malevolence, these lofty principles do not justify [the result].”) and
BENJAMIN KAPLAN, AN UNHURRIED VIEW OF COPYRIGHT (Lawbook Exchange 2008) (1966) (seemingly
conflating “plagiarism,” the norm against uncredited borrowing, with the legal offense of copyright
infringement) with e.g., Space Pirates, supra note 17 at n. 226 (considering various senses in which the word is
used, and specifying a meaningful usage) and Non-Neutral Principles, supra note 18 at n. 14 (specifying the term
in order to make it meaningful).

In addition to my core meaning of a person who commits a specified focal point offense, I can include
as a “pirate”, more generally, any person who infringes a trademark, infringes a copyright, or trespasses upon
some personal or property right. In all senses in which I use the word, a “pirate” is someone who has committed a
specified offense. But more particularly, when the offense is “merely” against a norm or against the law of nations

---

Notes:

262 Pirates and plagiarists are defined terms in my work. Supra note 133. I do not use them loosely as
some have done, but as specified words. Compare Graver Tank & Mfg. Co. v. Linde Air Prods. Co., 339 U.S.
605, 612-13 (1950) (Black, J., dissenting) (objecting to a very loose usage of the word “pirate”: “I heartily agree
with the Court that ‘fraud’ is bad, ‘piracy’ is evil, and ‘stealing’ is reprehensible. But in this case, where
petitioners are not charged with any such malevolence, these lofty principles do not justify [the result].”) and
BENJAMIN KAPLAN, AN UNHURRIED VIEW OF COPYRIGHT (Lawbook Exchange 2008) (1966) (seemingly
conflating “plagiarism,” the norm against uncredited borrowing, with the legal offense of copyright
infringement) with e.g., Space Pirates, supra note 17 at n. 226 (considering various senses in which the word is
used, and specifying a meaningful usage) and Non-Neutral Principles, supra note 18 at n. 14 (specifying the term
in order to make it meaningful).

263 In addition to my core meaning of a person who commits a specified focal point offense, I can include
as a “pirate”, more generally, any person who infringes a trademark, infringes a copyright, or trespasses upon
some personal or property right. In all senses in which I use the word, a “pirate” is someone who has committed a
specified offense. But more particularly, when the offense is “merely” against a norm or against the law of nations
magnets, plants deceptive addresses or magnets, or blocks or spoils addresses otherwise available, thereby effectively denying access, obstructing navigation, diverting information traffic, taking advantage of augmented presences, and destroying trust in cyberspace. There are also actors who are special targets for secondary liability, opportunistic plaintiffs who seek to lay off their costs of policing, and unexpected victims whose interests have as of yet been rarely, if ever, considered in the existing case law.

Part B of this section will deal with the costs reallocated among juridical actors. Juridical actors include practicing lawyers, clients, judges, clerks, professors, students, commentators, press and poets who deal with, decide, teach, explain or simply try to say something meaningful about mark-type conflicts in cyberspace.

Part C of this section will deal with the public. A full account of the judicial price of the focal point offense and the new likelihood of confusion factor must also weigh the effect on the public perception of the rule of law itself, and should offer some reasonable assurances it will not (as current approaches threaten to do) result in unexpected and costly errors.

A. Reallocating Burdens among Cyberspace Actors

Each of the persons affected by the focal point offense and the new likelihood of confusion factor is fairly burdened by the costs (and benefits) they provide. Therefore this system imposes no unbearable burdens on cyberspace. To the contrary, the costs are minimal and the benefits well exceed them. These are approximations, but they seem reasonable and useful estimates.

1. Surfers and Mappers

Mappers. The mapper is the indexer, the person who maps the Internet or the phone system. The phone system developed within a single-provider, regulated model, and the phone book was part of the system as it began. It is easy to forget how valuable the phone book was, or how coincidentally it developed. The internet demonstrates that there is nothing inherent in the architecture of navigation, and its history demonstrates what happens when there is no single registrar of addresses. On the Internet, this was once the old-fashioned “hit-or-miss” cataloger who simply listed registered domain name holders. It was once imagined there could it is often useful to call it a “piracy” offense. But when the offense is against a law, it is often more useful to name the law that has been broken (that is, the offense might be “trademark infringement” or “unfair competition.”) This avoids the temptation to engage in a question-begging exercise: calling someone a “pirate” does not necessarily mean the person has violated any law. It might be an expression of an argument that the conduct is contrary to law, a recommendation that the law should be changed so that the conduct will become contrary to law, or a normative desire that the conduct should be contrary law. It helps to indicate which sense is indicated, and I hope the context makes it clear which sense I am using.

264 Here I included not only asserted victims of some alleged pirate, but more importantly victims of the law itself: the vast unrepresented body of surfers who actually want to make nominative uses of markers in space in order to navigate.


266 One such service was (and still is) “WHOIS” by which a person could seek to establish “who is” the owner of a given Internet address. Some people might still remember that, on a lucky day and with enough time, there might be some successful navigation as a result. [update to the contemplated “thick whois” proposed in the May 2009 IRT/ICANN document, and suggest that even the whois will probably need an index]
never be a comprehensive listing of Internet resources anything like a complete phone book. Currently, this previously unimagined resource is supplied by the person who is the provider of the directory or the search engine and who thereby maps the previously unmapped domain of cyberspace. Focal points help the mapper either to pay for the directory or search engine, or to design algorithms to compile a directory or search engine in the first place. Without such a mapper, the Internet is not exactly useless, but is substantially less robust in terms of easy access, navigation, information and augmentation. Indeed, if anyone is essential to cyberspace, but also sensitive to, and threatened by the unsatisfactory state of the current law, it is the mapper. The new factor shifts the balance and permits value-added mapping by focal points with triggered ads to pay for the resulting hitchhiker’s guide when accompanied by reasonable technological accommodations, including notice, disclaimer, release/redirect or opt-outs.

Surfers. The surfer is the one who wanders into the code world and into cyberspace. Such travelers can have multiple characteristics. Some are entering for the sake of being there, and are concerned about access. Others are entering for the sake of exploring, and are concerned about navigation. Still others are entering in order to find out something, and are concerned about findable information. There are yet others who want to do something in space, and are concerned about augmentation and worried about the vulnerability of their augmented presence in cyberspace. The same person can combine interests, and shift interests so as to morph from one character to another while on the Internet or in cyberspace. If anyone has an interest to be considered in cyberspace, the surfer is one.

The leading indexer-mapper cases include some overprotecting, and some under-protecting focal points incorporating trademarks in space. Among the losers are the surfers in cyberspace. If the law overprotects trademarks incorporated into legitimate focal points in space, a surfer might lose the ability to navigate cyberspace to the extent the law impedes the ability of a mapper to create a search engine or directory, and to pay for it by targeted advertising keyed on trademarked expressions surfers use nominatively as focal points to describe the

267 Focal points can provide high value triggered, contextual keyword-driven advertising.
268 This is not to deny that other persons are also essential to cyberspace. Given that cyberspace requires a gateway, it should go without saying that the developers of the hardware and software tools that constitute the embodied switched network for moving information traffic, i.e., the computers, phone system, and network backbones are also essential. Without them there would be no access to cyberspace. But they seem well enough served by existing intellectual property specialties in trademark, copyright, patent and trade secret law, by the ordinary law of contract, and by basic norms and markets, as not to require separate treatment within the primary scope of this Article.
269 A prime example is Netscape (the targeted advertising case, involving a directory provider threatened because the case privileges marks in space by over-protecting them). See Space Pirates supra note 17 at ___. This result is adverse to a surfer because it threatens to deprive a surfer of useful and legitimate navigational markers in space partially paid for by high-value advertising.
270 The prime examples are Holiday Inns (a predatory, deceitfully designed trapping phone number) and 800 Contacts (a popup advertising case, probably involving a person not in the indexing business, decided on a rationale that would broadly exonerate indexers, but at the cost of under-protection to marks in space). See discussion supra note ___ and accompanying text; see also Holiday Inns, 86 F.3d at ___ (a typo-squatting case); discussion supra note ____ and accompanying text. While these results exonerate the focal point actor, they are adverse to a surfer because they will threaten navigation in cyberspace itself by abdicating legal regulation over invisible and attenuated uses altogether. By asserting such conduct is not even a “use” for trademark purposes, these cases threaten to overwhelm legitimate navigational markers in cyberspace by a combination of shear volume (chaff) and untrustworthiness (misdirection).
kind of goods or services they seek. If the law under–protects focal points, including those incorporating marks in space, a surfer might lose the ability to navigate cyberspace to the extent noise and deception overload the ability of addresses or magnets to function as effective focal points in space.\textsuperscript{271}

The new focal point offense and the new likelihood of confusion factor resolve both problems.\textsuperscript{272} Mappers and indexers provide focal point services in high cyberspace, their activities strongly support cyberspace, and the creation of maps and indexes are positive actions in cyberspace. The new factor allows these considerations to be an explicit factor in focal point analysis in a case where the mapper seeks to recover the costs of mapping by selling markers, or targeted advertising keyed to focal points, including those incorporating invisible or attenuated trademarked expressions. The new factor also allows these considerations to be balanced at the remedy stage, if liability is found, by providing a narrowed remedy proportionate to the harm. Such a remedy would often be limited to a disclaimer and perhaps a forced redirect.\textsuperscript{273}

The new factor should be a substantial benefit to the surfer, transforming and improving access and navigation at no direct economic cost to the surfer and with no foreseeable disadvantages to the surfer. The economic costs are shared by the offending actors. A proprietor of a site taking advantage of trademark-embedded magnets or addresses, the warehouser of a reserved site blocking access to trademark-embedded addresses, or a trapper diverting traffic would be required to install and maintain a notice, disclaimer, redirect or opt–out. Such costs will likely be relatively small. Any offending user whose marginal costs of their cyberspace intervention cannot bear such modest additional costs will be one whose contribution to cyberspace was almost certainly negative or non–valuing adding in the first place.\textsuperscript{274} If, and to the extent there are certain affected cost–bearers who present special circumstances, the flexibility of the common remedy will allow a juridical agent to shift some or all of the cost of the remedy to the mark proprietor.

The mapper’s cost–absorbing problem deserves some discussion. A mark proprietor should be able to gain satisfaction from the directly offending party. In the case of magnets or addresses leading to a third party site, including by keyword triggered ads, the mark proprietor could require the offending conduct be resolved at the offending site itself. It should follow that the mapper would be only secondarily involved. Perhaps the targeted keywords offered for sale by the

\textsuperscript{271} The current law has been deaf, dumb and blind to the interests of the multitude, not only of consumers, but also of non–consumers and others who enjoy cyberspace. Surfers need a map, and they like to use magnets and addresses to navigate. The law seems a bit condescending to declare the surfer is likely to be confused simply by being provided with the information that the surfer is seeking. An explanation for this is not necessarily that the law is unaware, but that there are institutional, systemic barriers to rational juridical decision making and thus no way to handle the problem under current approaches to it. See discussion supra notes. __–___. Other proposals to solve the problem of marks in space require information that is not readily attainable for judicial proof, see notes ___. This Article proposes that the law take advantage of the architecture of cyberspace and force the code in the direction of polling. As a result, there will be no need to guess any surfer’s interest, nor to pin any surfer down to a single, invariant interest. Under the new approach, there will finally be relevant evidence upon which to base a rational decision.

\textsuperscript{272} See discussion supra notes __–___ and accompanying text (the balance between over– and under–protection). The new factor can be expressed in both a generalized form (“nature and place of use”) and as a more fully specified factor, supra note ___.

\textsuperscript{273} See discussion supra notes ___.

\textsuperscript{274} It would certainly seem fair to make the presumption that the use is negative or non-value adding.
mapper could be compartmentalized: the *Netscape* keyword set might, for a first price to the prospective advertiser, include only those nearly 400 words excluding trademark terms and, for a second price, include all those plus the two trademarked keywords. The mapper offering to sell and the advertiser considering whether to buy, and at what price, could gauge whether the inclusion of the trademarked keywords would be worth the expenses of tracking, monitoring and placing the required antidotes (the notice, disclaimer, redirect or opt-out) in light of currently available technology. If the effort were worth the price, it would occur. Otherwise it would not. Regardless, the cost would be borne by those creating or contributing to the cyberspace intervention (the focal point offense), and at a reasonably predictable price from the prospective vantage point necessary to permit an efficient allocation, independent of hindsight or backward-looking juridical risk.

2. Spoofers and Trappers

*Trappers.* The trapper is the person who takes advantage of the map of cyberspace, including in the broadest sense someone who takes advantage of a sort of Nash equilibrium by appropriating anticipated focal points associated with vanity addresses. Once it became a shared belief that providers of goods and services would be findable in cyberspace because they will include their trademarks as navigational markers embedded in addresses or magnets placed in cyberspace, then vanity addresses and hidden magnets which include trademarks became valuable as dynamic information apart from, or in addition to their value as “goodwill” or their value “as” a mark. They are associative focal points. The trapper trades on the value of the commercial persona of a provider of goods and services by taking an associated trademarked expression, and placing the expression inside an address or magnet as a dynamic focal point. The reason this person is called a “trapper” is because the incorporated trademark does not belong to the trapper, but is being placed in cyberspace by the trapper in order to capture or ensnare traffic intended for the proprietor of the mark. The trapper thus preys upon those who have assumed the way to find a commercial provider in cyberspace is by guessing at an address or magnet as a focal point incorporating a trademark associated with the provider. Consider the case of “superman” if its

---

275 See Folsom, *Missing the Mark*, supra note 16 at ___ (observing the number of trigger words were nearly 400, of which only two raised trademark objections from a mark proprietor: perhaps there were others not yet before the court, but surely they could be handled in the same manner).

276 The solution proposed by this Article offers the advantage of transactional simplicity. It is meant to appeal specifically to practical lawyers who seek to give practical advice to clients. A rule that is relatively clear, and with costs of compliance (or non-compliance) that are ascertainable, is a rule of thumb that might encourage transactional lawyering more effectively than is possible in the face of too much uncertainty.

277 Where people must decide on action in the face of uncertainty, based in part upon how others are likely to act, and how they themselves might obtain more information, various strategies or plans that specify the action to be chosen can be developed. As such strategies develop, certain of them become dominant, and a strategic equilibrium might arise. The “Nash equilibrium” is one in which certain beliefs and choices of actions reinforce one another and persist; sometimes a particular equilibrium arises if there are shared “focal points” or beliefs about behaviors that have psychological relevance. See HOWELL JACKSON, ET AL., *supra* note 30, (introducing a common approach to game theory suitable for general use by juridical agents who might not otherwise be familiar with it). To the extent trademarks serve as focal points in cyberspace, they take on an additional value. The question is: who gets to appropriate, expropriate or otherwise influence the value of a mark “as” a focal point. This is one more problem the proposed new factor is designed to solve.

278 If the only magnets or markers that existed in cyberspace were vanity addresses, and if there were no
artificially-induced scarcity value\textsuperscript{279} were removed by an effective redirect. With an effective redirect in place at the trapping location, then any arbitrary expression, regardless of its ease of memory, and regardless of the accidental historical development of vanity addresses and substitutes for vanity addresses on the internet side\textsuperscript{280} and on the phone side\textsuperscript{281} of cyberspace, would become just as valuable to the person with whom the marker is associated as the genuine focal point itself. In such a case, an expression like “mxyztplk” becomes as valuable to the proprietor as “superman.” This is because what remains in the hands of the trapper is no longer simply “superman” incorporated in a dynamic focal point, but “superman” accompanied by a technologically effective redirect. There is no requirement that focal points be accompanied by notice, forced redirect/release, and like measures, then those users looking for a location whose address they didn’t already know would focus their search on vanity addresses, creating a value opportunity for economic rent-seeking activity by a trapper.

\textsuperscript{279} In this example, we will assume “superman” is a focal point related to the branded “superman” character owned by DC Comics or whomever the successor in interest might be—the beauty of the redirect remedy which is part of my solution is that the searcher need not bother with looking up the current name of the proprietor: the redirect will take care of that. If the only way to find Internet information about “Superman” were by a vanity address, then the search strategy might include looking for http://comics.com, http://dccomics.com, or even http://comics.com or http://superhero.com, thereby creating a commercial value in a mere vanity address. There are, of course, at least two other regimes, both involving externalities, that offer substitutes for such hit-or-miss address searches: (1) an address/key/index, like the phone book that was given away free as a loss-leader by the phone utilities as the phone system got off the ground (and/or as required of them as regulated utilities), and (2) a search engine driven by indexed terms, and not limited to the narrow and small set of vanity addresses used as magnets — so that “superman” keyed into, say, a GOOGLE-style search engine would eventually draw a searcher to the right destination regardless of address. See generally Feist Publications, Inc. v. Rural Telephone Service Co., 499 U.S. 340 (1991) (illustrating how the phone book itself becomes an almost accidental object of value to its creator). If there had ever been a plausible phone book to the Internet at the time of its creation, it seems Internet vanity addresses incorporating a limited number of trademarked terms would not have had quite the value they once commanded. But such a phone book would have been unimaginably unmanageable, hence the odd distortion that permitted temporary opportunities for arbitrage in respect of vanity web addresses until the old-fashioned law caught up.

\textsuperscript{280} Given the perhaps unexpected creation of a strong and viable search engine and directory system after the Internet was already well-established, it would seem that (if spoofing, detours and other piratical conduct involving trademarked terms could also be discouraged, as they are under my proposed solution) an Internet vanity address containing a trademarked expression would become largely irrelevant as a way to guess an unknown Internet location (IP address) of the proprietor of trademarked goods. One might imagine a time in the future (after the proposal of the Article is adopted) when a search on “superman” would provide useful information (because of required notices or redirects), able to lead a surfer to a web site sponsored by the proprietor of the original trademarked superman character, even if the mark proprietor did not own the vanity address and were using a totally irrelevant or impossible to remember web address (say, http://mxyztplk.com). See infra note 289. As the practical value of mark-based magnets comes to exceed the practical value of mark-based vanity addresses, the commercial value of a vanity web address containing a trademarked term might become negligible to anyone other than the trademark proprietor, or to persons who can still draw traffic after having re-pointed all incoming traffic to the mark proprietor. At least the non-mark owning registrant of such a vanity address would not be expropriating the proprietor’s mark nor appropriating the value of the goodwill associated with it, but would be dealing with users who had deliberately chosen to deal.

\textsuperscript{281} Because of the different architecture of the phone system compared to the Internet, it never happened that a person wanting to call a particular individual would think to dial, say 1–202–SandraDayOConnor (perhaps for more information about Feist, supra), or that a person looking for the Ford Motor Company would ordinarily think to dial, 1–248–FordMotorCompany. Of course, as it happened, the standard U.S. phone number is of a determinate length that does not permit such customization, and the guess-work for truncated pneumonic numbers would probably not be worth the effort (would it be “1-202-SandDa”?, would it be “1-202-OConnor?” or something else? and what about all the others sharing the same last name?) By the same token, would it be 1-248-FrdMoCo? Instead of trying any such strategy, the searcher would simply use a phone book or other directory because the phone system had already been mapped, as it was created, and because the architecture or code of the phone system limited the universe of U.S. phone numbers to seven characters after the area code (1–202–OConnor exhausts the character field, before exhausting the population of all persons having the same last name within the calling area) and so prevents the sort of fine discrimination by vanity number that would have been necessary to use vanity phone numbers as focal points for efficient searching strategies.
longer any economic rent in “superman” in the hands of a trapper. Accordingly, the users of any “superman” focal point will be confined to those who can still prosper even when everyone drawn to the focal point may easily and almost effortlessly go somewhere else because of the presence of the redirect which points to the location of the genuine focal point association.

**Spoofers.** The spoofer is the person taking advantage of the map to cyberspace by pretending to be of more interest to the mapper than is the case. Once it becomes known the search engines have programmed spider software applications to crawl through cyberspace, it becomes possible to guess how the spiders have been programmed to rank sites. The value of a search engine to surfers, and hence to potential advertisers, must be related to its ranking algorithms. If a surfer is to invest any time in, or develop any loyalty to any particular search engine, the searcher must get an average response from the search engine more or less close to what the surfer is seeking. The programming, including what has been called the artificial intelligence of the spiders, is one factor differentiating search engines from one another.

A spoofer complicates the navigational problems a search engine is designed to solve. If a given spider’s algorithms became known, or if they are reverse-engineered, then a spoofer could mimic the signs returning a hit and leading to a high relevancy ranking. The measure–countermeasure, or servo–mechanism reaction resulting from this is part of the story of the continuing refinement of search engines. To go back to a simpler time, suppose a spider were programmed to rank the relevance of two sites by giving weight to the relative number of times a search term appears: if a searcher were seeking “Ford” then the site including the term ten times might be expected to be more relevant to the surfer than the site using the term only once. As this logic becomes known, then a web site designer who wants to help a client attract traffic will be able to spoofer the search engine by including the term “Ford” in meta–tags invisible to a surfer, or in hidden text likewise invisible to the surfer, multiplying the number of inclusions and catapulting the site towards the top of the relevancy rankings. While amusing, the cases wink at the fact the spoofer is spoiling the business of the mapper with the intent of fooling the surfer, while simultaneously deliberately undermining the foundational values of cyberspace and polluting the commons.

The cases dealing with trappers and spoofers suffer from being under the domination of cases either over-protecting marks in space, or under-protecting marks in space. Beyond that, the existing law has no particular set of tools 282

---

282 It is beyond the scope of this Article to speculate about a cause of action by an indexer against a spoofer, but a spoofer who spoils the search engine’s value would seem to be engaging in the sort of waste, rather than competition, that courts have been able to discourage without preventing robust competition. *Compare RESTATEMENT, supra* note 96 at § 1 (stating the general rule of free competition without legal liability) *with id. cmt. c. (discussing the relevance of evidence of ill will or malicious motive, at least to merit heightened scrutiny of the actor’s methods under various rules) & d. (recognizing principles of deceptive advertising); and see id., ill. 7 & 8 (suggesting liability, under ordinary principles of unfair competition law, in situations that resemble the sort of spoofing which can occur in cyberspace). *See also the maxim: sic utero tuo ut alienum non laedas* (one must so use his own [rights] as not to interfere with [the rights of] another), William Alfred’s Case (9 Co. Rep. 59a), reprinted in *THE SELECTED WRITINGS OF SIR EDWARD COKE* 312 (2003) (__) (adverting to the “fetid filth and other muck” flowing out of the offending property and as a result of which a neighbor “for a long time did not dare to remain in his aforesaid mansion house for fear of infection by the horrid stench of the smoke, filth and other muck, etc.”)
available by which the cases can be sorted. The focal point offense and the new likelihood of confusion factor provide such a tool set. Trappers and spoofers both operate in high cyberspace and their activities strongly impact cyberspace. The effect of the trapper is not positive, but negative. The effect of the spoofer is less obvious, but leans towards the negative or neutral at best. The existence of the focal point offense and the new factor will allow a meaningful inquiry, which in turn will develop the information to determine on a case by case basis the impact of spoofing.

Moreover, if there is liability for trapping or spoofing, the focal point offense and the new factor will guide a decision maker in tailoring the appropriate remedy, including disclaimers and forced redirects. Significantly, the focal point offense and the new likelihood of confusion factor are general enough they can be expected to be technology-independent. The costs will be allocated to the spoofers and trappers because the remedy requires them to insert, maintain and guarantee effective notices, disclaimers, redirects and opt-outs within their own domains. If the relatively modest costs of self-policing drive some spoofers and trappers out of the “business” of fooling others, the economic cost to the surfer and to the public interest is nothing (zero), and there is, instead, a positive benefit to the public.

3. Spoilers and Arbitrageurs

_Spoilers_. The spoiler is the person who wastes another person’s mark in cyberspace. On the Internet, there are, or from time to time have been a limited number of markers serving as attenuated addresses including trademarked terms. The limitation is a function of an underlying architecture combined with focal points. Apparently, there was once a time when some non-trivial number of surfers looking for “Ford” cars or trucks or SUV’s would have guessed to type:

---

283 The solutions proposed here are technologically aware, but not technologically dependent. So it can handle a web 1.0 or web 2.0 (or a web 3.0) set of circumstances; and it can handle domain names when there have been a limited number of gTLDs, an expanded number of gTLDs, and an unlimited number of gTLDs. If there are only a few effective focal point addresses in any place within cyberspace, or if there are many, the focal point offense and its limited common remedy still applies because it is scalable to the nature of the offense.

284 This is a perhaps anomalous if not unexpected instance of the opportunistically rivalrous use of an otherwise non-rivalrous good. Of course marks are ordinarily “rivalrous” in the sense that the more one person uses another’s mark so as to cause a likelihood of confusion, the less goodwill remains in the mark. _Cf_. LANDES & POSNER, supra note 129 at ___ (expressing the more conventional formulation). But the mark itself in ordinary space is “non-rivalrous” in the sense that ordinarily, no amount of use or registration of an expression by one person can actually prevent anyone else from using the expression (the other user might incur liability, but there is nothing whatsoever in the nature of things that physically prevents another user; especially is there nothing comparable to a junior user preventing, wasting or spoiling the opportunity of the senior user to use its own mark by a prior registration of it). It is an unconventional word usage to describe the preemption of a senior’s mark in cyberspace by a junior as somehow converting the use of the expression itself into a “rivalrous” use of an otherwise “non-rivalrous” thing, though that is exactly what is happening—and that that is why this Article describes the offending activity as an “expropriation” or as a “divesting” use. It is this expropriation of a senior’s mark (and associated goodwill) by a junior that is wholly without parallel in ordinary space, at least in the United States. It would seem startling that a junior user could preempt a senior user from using a source signifying expression (the senior’s trademark) in some medium simply by being the first registrant or even the first user in that medium. This would be as strange as if the first user who got a placement of “Tide” on the television could have prevented Proctor & Gamble from effectively getting its brand on television in a place where viewers would have expected to see it. The proposed solution of this Article explicitly confronts the problem of expropriating and divesting uses in cyberspace. If, in fact, there really is no existing principle of ordinary trademark-related law that can reach this sort of misappropriation, _but see supra note ___, then here (at least) is an occasion in which cyberspace needs a law of cyberspace that is adapted to its (apparently) unique architecture compared to ordinary space.
http://www.Ford.com, or tried the combination http://www.FordMotor.com http://www.FordMotorCo.com or http://www.FordCars.com (or “something else.com,” or “.net” and so on) until they got connected to a “Ford” motors website. Perhaps the only significantly likely focal point is the first one in the above set.285

There being, perhaps, one and only one best, most efficient or “game optimal” or suboptimal way to get to the “Ford” website, if someone else got there first by registering that one domain name, then Ford Motor Co. would be forever precluded from efficiently expanding its reach from ordinary space into cyberspace. Hence, were there no law to prevent it,286 a spoiler could expropriate or waste the goodwill associated with a mark by precluding its use by Ford Motor Co. as an efficient focal point–solvable address in cyberspace unless Ford were prepared to buy its own goodwill back from the expropriating user.287

Much of this was changed by the introduction of search engines at no direct cost to the surfer. Now, all a surfer must do is to type “Ford” into the search window and then scan a list of sites, one of which will probably include the Ford Motor Co. and others of which might include the Ford Modeling Agency and many other potentially relevant “Ford” entities.288 Only one of these could have been the prime focal point address so desperately coveted back in the pre–history of the Internet, as described in the leading cases.289 If a “thick” who–is should ever be created,290 it might shift the nature of the focal point offense, but is unlikely to resolve such offenses (the new “who–is” may well be not only subject to spoofing and spoiling but also cumbersome to use), and the new focal point offense is very

285 It would seem the other choices would involve too much guess work to make them likely candidates for an efficient search strategy.

286 This Article contends that ordinary principles of trademark–related law, as adapted or transformed for cyberspace in a new “nature and place of use” likelihood of confusion factor, should constrain such behavior. This Article recognizes that various ad hoc special statutes have been enacted to handle such conduct, but this Article contends that those ad hoc responses are unsatisfactory: they are too sporadic, easily circumvented and too slowly revised or re–enacted to catch up with circumvention, and the various regimes are not well coordinated with each other. See supra notes ____.

287 By “focal point–solvable” this Article simply means it would be a good guess by someone who didn’t already know how to find the provider in cyberspace. See supra note ___. infra note ___. (this is non–complex game theory language).

288 There might be a President Ford library, or perhaps information about the person who shot Jesse James, or information about any number of others who bear the same surname, but all or most would be fairly findable through the search engine, and the Ford Motor Co. would probably be findable among all these others by the surfer who was looking for it (assuming there were no one spoofing the search engine and assuming the search engine were reasonably robust).

289 It would seem that the commercial value of many vanity web addresses containing trademarked terms would decline as, and to the extent that, a person guessing the Internet address of a mark provider or sponsor could simply use a magnet–based search strategy to input the trademark, rather than an address–based strategy to input possible trademark–containing domain names. The proposed solution would transform the architecture of cyberspace to do just that. See supra text at note 280 (suggesting http://mxyztplk.com could be almost as valuable to DC Comics, if that were the proprietor of the superman mark, as the vanity address http://superman.com —or at least no less valuable than the vanity address— if the common remedy will require a search engine to direct a surfer to the sponsored site, or if it will result in a redirect to the sponsored site, regardless who takes up the vanity address in the first place). If, pursuant to the focal point offense and the new factor proposed in this Article, the surfer is provided with a fair opportunity to reach the mark proprietor’s site, the goodwill value of a vanity address will be stripped from the overall value of the address, perhaps driving its price back down more nearly to its cost and removing the artificial incentive to economic rent–seeking activity that might still inhere in the present system.

290 See [the ICANN proposal, as floated by the IRT in anticipation of the roll-out of the new unlimited top level domain names].
likely to be suitable even if the world wide web should ever come to resemble the telephone system, accessible by a directory (a phone book) rather than by a search engine.

There is, however, more than one type of spoiler. As we have already seen, one type wastes by taking prime focal point vanity addresses out of the hands of trademark proprietors (warehousing them without making any “use” of them as markers at all).\(^{291}\) Another type of spoiler places detours or roadblocks. Some spoilers might actually use the domain name as a marker, but in a spurious or illegitimate way constituting a detour to most surfers.\(^{292}\) All spoilers interfere, and under the new factor each bears the cost of the solution: providing notice, disclaimer and a redirect. If neither type of spoiler contributes anything of measurable value in excess of the modest cost of remediation,\(^{293}\) then both constitute a negative influence on cyberspace and the loss of such spoilers is one the public would welcome, and about which the spoilers would be ill–advised to complain.\(^{294}\)

**Arbitrageurs.** The arbitrageur is yet another person drawn to economic rent-seeking activities in cyberspace. One form is the crude example occurring in the early days of the Internet, the commodity being prime focal point domain name registrations, including trademarks embedded in domain names at the “.com” and “.net” and “.org” top levels, perhaps accompanied by common corresponding trademark typos at the same levels, any of which could be purchased for a small annual fee. Markers such as these would bring a much higher price in a different

---

\(^{291}\) This is the difficult “use” problem, if there is one, in cyberspace, see supra notes ___ (describing the general problem of invisible and attenuated “uses” in cyberspace). Some cases have struggled to find that a domain name registration containing the trademark of another person, even if only warehoused and not made “live” on the Internet, can still constitute a “use” sufficient to cause a likelihood of confusion. See supra note ___. That is not an impossible finding, and may even be correct, but the new factor frees a juridical agent to see more clearly (a) that the offense is expropriation of another’s mark by a divesting use of it, and (b) that the remedy is to require the site be made “live” and that it contain a notice or a redirect to the mark proprietor. The modest remedy is exactly appropriate to the offense, and both the finding of liability and the measured remedy are within the authority of a juridical agent to compel. See supra note ___.

\(^{292}\) This section concerns a “spoiler” who has no legitimate claim on the expression. The new factor disarms the spoiler by requiring a notice, redirect or release. At the same time, the new factor handles equally well the prior claimant to the address who does have a legitimate claim, see supra note ___. (e.g., the Ford modeling agency, or the President Ford library). The same notice, redirect or release can enable surfers to find other focal point–type claimants to the expression and to any mark incorporated therein. The convention would provide for redirects among multiple mark claimants, all to the benefit of surfers, and all by way of reasonable technological accommodations. This is because the architecture of cyberspace permits changed code to change the results without inefficient or wasteful efforts, and the new factor takes advantage of the opportunities presented by the architecture of cyberspace to make it work better.

\(^{293}\) If the spoiler still does have some value beyond the cost of remediation, one would suppose the spoiler would remain active at the offending site to service some number of surfers who, having been notified how to find, or having been redirected to the mark proprietor, nonetheless want to transact business with the spoiler. Yet another advantage of the solution proposed by this Article is that it broadly enables all interests to coexist, provided there is disclosure. This solution effectively polls all the concerned actors at the point of the offending conduct, and relies on the actors to find their desired locations rather than relying upon ex post juridical guesswork to attempt to determine what the actors were trying to do.

\(^{294}\) The spoiler who is adding no value, but who is disrupting navigation in cyberspace or expropriating another’s mark would seem, by the very act of complaining about the requirement that it place a notice or redirect, to convict itself of fraud, consumer deception or unfair competition. This would seem to a self–correcting feature of the new factor.

\(^{295}\) In this context, a “focal point” is an estimated location of an address in cyberspace, in the nature of a well–informed guess likely to be shared by others who will make the same guess. See supra note ____ (more generally, it may be thought of as a “Nash equilibrium” game solution).
market (the resale market formed by selling the trademark’s goodwill captured in
the domain name back to the trademark proprietor, or else to market–making
brokers at a price to be named, but significantly higher than the relatively low cost
of the domain name registration itself).

A second and more interesting form of profit-taking is the opportunity of
aggregating information and selling either information or brokerage services tied to
that information. An insurance broker might simply place magnets including
trademarked designations owned by the various insurance companies whose
policies the broker handles. A travel agent might place magnets including the
hotels, or airlines, or rental car companies with whose products the travel agent
deals.296 A consumer’s guide might place magnets alerting its readership to topics
covered by the guide, keyed to trademarks owned by the persons whose products
were reviewed. Finally, some members of the same set of users (insurance brokers,
travel agents, consumer’s guides, etc.) might go beyond the use of a trademarked
term as a magnet, and actually appropriate one or more trademarked terms as part
of an address.297

All of these arbitrage activities take place in high cyberspace, and all of them
strongly implicate the values of cyberspace. Some of these actions are positive,
some are negative and some are neutral. The current cases lack any principled tool
for distinguishing one from another. The new factor supplies the missing tool. An
arbitrager in the class of information aggregator or broker might be more liable to
a reassignment-type remedy for an attenuated cyberspace intervention if the
offending use were in an address298 than if it were merely in a magnet.299 At the
level of magnet only, the remedy might require little more than a notice, disclaimer
or redirect. The focal offense provides a fast and accurate remediation. The new
factor for residual trademark infringement cases not only permits, but invites easy
analysis of the relevant circumstances as an explicit factor in an attenuated
likelihood of confusion analysis where an arbitrager seeks to profit by trafficking
in invisible or attenuated trademarked expressions “as” markers. The focal point
offense and the new factor for likelihood of confusion allow these considerations
to be balanced at the remedy stage by providing a common remedy proportionate
to the harm. Such a remedy could often be limited to a disclaimer and perhaps a
forced redirect/forced release. The costs would be borne by the offending parties.
This seems appropriate. The offending parties, after all, are the ones creating the
attenuated confusion and diminishing the value of cyberspace.

The spoiler cases are more difficult to handle under ordinary trademark
analysis because “pure” spoiling, as by warehousing alone—registering, but
neither using, selling nor offering to sell a trademark-containing domain name—
does not seem to be conduct causing a likelihood of confusion under ordinary
principles of trademark law.300 But because pure spoilage constitutes a cyberspace

297 See Holiday Inns, 86 F.3d at
298 Cf. Holiday Inns, 86 F.3d 619 (the offending use was typo–squatting on an address in the form of a
vanity phone number, and in which the analysis available to the decision maker at the time resulted in a finding of
no liability) and discussion supra at section II (resolving Holiday Inns as a focal point offense).
299 Government Employees, 330 F.Supp. 2d at ___.
300 Cf., e.g., Panavision, 141 F.3d at ___ [conform short names, Toeppen (?)]; see discussion supra note
intervention—it is a focal point offense—the new analysis cooperates with other legal domains, including ACPA, UDRP and unfair competition to provide an easy and rapid resolution with a reasonable remedy.\footnote{The common remedy is one that is a reasonable technological accommodation to the mark proprietor. If the trademark approach would lean towards reassignment of the offending expression to the mark proprietor, but only upon a finding of likelihood of confusion, an unfair competition approach might lean towards a required disclaimer or redirect. That is, if an actor has registered and warehoused a domain name containing the trademark of another, then it would be reasonable to require that actor to provide a web site notice and redirect that would be triggered by a search on the spoiled mark. It might be to this effect: "you have entered an expression that is a trademark owned by X; but X is unable to operate a web site at that address because Y has blocked X from doing so even though Y doesn’t maintain any web site at that address either. Click [here] to reach X. Click [here] to reach Y."}

4. Shills and Advertisers

\textit{Advertisers.} Advertisers seek to make consumers aware of goods and services and to turn non-consumers into consumers by making them aware of a need or desire satisfied by the goods or services offered. Many consumers in ordinary space are on guard against advertisers, mostly because ordinary market constraints and norms create customary zones within which persons might be on notice they are about to be exposed to advertising.

Cyberspace permits invasive techniques, not only at the level of keyword triggered advertising by a user who is actively shopping or searching for information, but it sometimes permits such techniques to be aimed at someone not actively shopping or alert to the intrusion. Such ambush-style user profiling, content-creation and insertion into a user’s cyberspace experience presents more than a potential for harm. The metaphor is not that the invisible use constitutes activity “like” merely thinking about a mark,\footnote{Cf. Contacts ___ at ___ (using the metaphor, in a case involving an intrusion into a user’s computer) [cross ref the psherspace examples, supra].} but that it more nearly constitutes someone else intruding into the thinker’s consciousness.

One new angle on likelihood of confusion is the likelihood of mistaking the invasive source or impulse for the thinker’s own. Against this harm, the new factor explicitly allows an approach permitting advertising but protecting against invasive advertising. The remedy includes notice and might include opt-outs in the appropriate case. The flexible remedy answers the need for advertising to pay for certain services and resources in cyberspace and to respond to the public interest in maintaining a robust cyberspace, while also discriminating against predatory or invasive advertising. In the case of advertising, the cost is notice or opt-out. Even here, if there are significant numbers of users who value such intrusive advertising as to not opt-out, then to those users the “services” will remain available. The costs will be borne by the advertisers and will not adversely affect either users generally or those particular users who might value them.

\textit{Shills.} While many persons put up with commercial advertisements as a bearable burden providing a benefit, few persons have any need of shills. The shill is a decoy or an accomplice posing as an enthusiastic customer to encourage other buyers; a person who poses as a disinterested advocate of another but who is actually the other’s party, mouthpiece or stooge.\footnote{OED online (second edition).} It is hard to imagine any value-
added services from this quarter. The new factor provides a tool to dissect advertising in cyberspace. Once the costs of notice, disclaimer, redirect or opt-out are imposed, shills will not survive such costs and their “business” models might collapse. Once again, this is a cost borne by the offending party. It is a net benefit to the public interest. In the unlikely event anyone actually wanted to be duped by shills, such an actor could elect not to opt-out, and the group of such persons might support the shilling business. Meanwhile, surfers, shoppers and legitimate advertisers could go about their way in cyberspace free of these intrusions.

5. Shoppers and Consumers

Consumers. At the outset of this subsection it is useful to identify an equivocation. In some sense, everybody in cyberspace is “consuming” something, if only cyberspace access itself, when they are in cyberspace. In this sense, surfers and mappers are consumers, and in this same sense information-seeking activity is engaged in by consumers of cyberspace. In another sense, some persons are actually “shopping” for something other than cyberspace access or information itself, so they may be thought of as consumers of the goods or services they seek to find and purchase by way of cyberspace. The new factor helps to distinguish shoppers from consumers in these senses. It re-emphasizes the concern of trademark law with likelihood of consumer confusion, but in cyberspace it is too easy to mistake “mere” surfers for “consumers” of a product other than cyberspace itself, and to forget that perhaps the core concern of trademarks in cyberspace might be with surfers actually shopping for goods or services offered, produced or sponsored by someone. By distinguishing “shoppers” from “consumers” the new factor provides yet another clarification useful in assessing the real relations in cyberspace.

Shoppers. There are at least two types of shoppers. In the first case, shoppers elect to use someone’s mark as if it were a nominative for a product category—electing to take someone’s trademark and to use it as a dynamic focal point. It would seem no one can or should be able to stop anyone in this context from using any word, including a trademark, any way they please. But there is a second case, when a person uses the Internet simply to effect a transposed ordinary space transaction in respect of any already known brand. That is, the person is neither comparing nor playing, and is not interested in bouncing around from site to site, nor in pursuing every rabbit trail or interesting hint or clue. They just want to buy a shirt from a known and preferred vendor. Instead of driving or walking to L.L. Bean or Land’s End the consumer wants to get there as an augmented presence by phone, or on the Internet, and wants to do so quickly and without any waste of any time. Instead of finding out everything or anything about shirts, other shirt

---

304 If there is ever any legitimate place for a “not-using-as—a-mark” this would, perhaps, be it. The consumer can use anyone’s trademark anyway she pleases. Of course, when the consumer deliberately uses the mark “as” a focal point, the more obvious and direct solution might simply be to remark that the consumer couldn’t possibly be confused, or else to conclude that the expression simply hasn’t come to be associated with any particular goods or services (it might not even be a mark if consumers see it simply as a focal point, though it might be better candidly to acknowledge that a mark can also be a focal point, and it just depends upon the context).
providers, the history of shirts, or complaints from disappointed prior customers or others who have some axe to grind or story to tell, the shopper just wants to buy a shirt as rapidly as possible.

When it comes to translating the real relationships of real persons in cyberspace into the language of legal category, it is only the second kind of shopper, most like the hypothetical reasonable consumer, who is the driving force in the “likelihood of confusion” analysis. This insight is yet another the new factor facilitates. Whether a “surfer” is likely to be confused or not is a difficult question, but more importantly, it is a different question from whether a “shopper” is likely to be confused. Not all surfers are shoppers. Nor are all “consumers” in cyberspace shopping for goods or services. Some consumers of cyberspace are merely surfing, not shopping. Some shoppers are comparing, deliberately using marks as nominatives. They are the wrong population to sample.

The focal point offense and the new factor are designed to protect all shoppers, not least by identifying their interests and distinguishing them from the interests of other factions in cyberspace. Because there is a flexible common remedy accommodating the different factions in the public interest, the costs of the focal point offense and the new factor are transparent to these factions. If the offending party provides the suitable notice, disclaimer or redirect, the surfer who “consumes” cyberspace by following navigational markers into obscure corners is not burdened, and neither is the comparison shopper. But at the same time the already-decided shopper who is attempting to become a consumer of particular branded goods or services will (by virtue of the same notices, disclaimers or redirects) be able more readily to avoid those obscure destinations and instead more rapidly find the mark proprietor. This is exactly what marks are intended to do. It maximizes search cost efficiencies. The focal point offense and the new factor obtain this result at modest cost to all parties, with the cost being borne by offending actors (or allocated between offending actor and mark proprietor) and with the benefit being available to shoppers and surfers alike according to how they react to the notices and redirects and with no burden to either shopper or surfer.

6. Competitors and Mark Proprietors

Competitors. The competitor, or other offending actor, is the person less invested in any of the other roles assumed in cyberspace (neither surfer, mapper, trapper, spoiler, or any of the others), but is more directly interested in marketing goods or services more or less closely related to those of the proprietor of some trademark. They may do so by way of a designation used as a focal point in a cyberspace intervention causing an invisible or attenuated likelihood of confusion with the proprietor of a trademark, or by expropriating another’s mark. In cyberspace, a competitor includes any pirate (as defined herein) tampering with the map to cyberspace by way of trademarked expressions used as markers and spoilers, always for some purpose relating to some project, goods or services of the

---

305 These would include goods that are complementary or substitutionary to those of the mark proprietor [Landes & Posner], and in cyberspace would include the medium of cyberspace itself as a zone of expansion for marketing goods or services.
proprietor rather than the mark proprietor.

**Proprietors.** The proprietor of a trademark, it should not be forgotten, is the one who first used a distinctive designation to identify goods or services sold or offered for sale in the ordinary course of business and to distinguish those products from other producers or other sponsors. By such association of the designation with product and producer (or sponsor), the proprietor has created goodwill value both to the proprietor, consumers and potential consumers. Moreover, by such association, the proprietor assists the public interest in preventing others from engaging in offending conduct causing a likelihood of consumer confusion with the proprietor’s mark used in connection with those goods and services.

The consumer (shopper in cyberspace), proprietor and competitor are the ordinary subjects of ordinary trademark law. A last, but not to be overlooked, advantage of the focal point offense and the new likelihood of confusion factor is that they do not reinvent the wheel, nor do they elbow aside ordinary trademark law because of some undefined mumbo–jumbo about an imaginary thing called cyberspace. Where ordinary principles of ordinary trademark law can do the job in cyberspace, the new factor invites them to do so. The focal point offense and the common remedy remain, however, as useful guides to ensure trademark law does not wreck the Internet, the phone system or cyberspace by accident, and that it does not disfigure the law itself by some sort of bleed-back doctrinal creep or reverse doctrinal creep from cyberspace into ordinary space. The cost of a reasonable technological accommodation to the trademark proprietor providing a notice, disclaimer and a redirect to remedy a cyberspace intervention is a cost that can and should be borne by a competitor initiating the act. Once the modest cost has been accepted by the competitor, all other participants in cyberspace, and the public interest, will be enhanced.

The focal point offense and the new likelihood of confusion factor permit and invite consideration of the obvious interests of consumers (shoppers in cyberspace), proprietors, and competitors, but also permits and invites a healthy consideration of persons other than shoppers, proprietors and competitors. It not only tests for whether the parties involved are shoppers but takes the public interest into account. It is well known some (surfers) are not bothered by, and welcome, a great deal of information; yet others (shoppers) are frustrated and perhaps likely to be confused by the same information. Both of these may be considered “consumers” of cyberspace, but the shopper is the prime object of trademark law’s concern. Rather than bog down in an uncertain and unknowable debate over what “consumers” (or “surfers”) want, as if anyone could know, or as if any one user

---

306 It ends the blindness of current law, which is unable to distinguish the typical conflicts that occur among the characteristic users of cyberspace. Because the same person is sometimes in the position of a consumer, sometimes a surfer, and always an augmented presence in cyberspace something is lost in the blind translation from ordinary space to cyberspace. The new factor recovers the lost balance in cyberspace by providing a mode of discussing what is actually happening among the users there.

307 Ordinary trademark law does not deal with likelihood of frustration, or likelihood of inconvenience. Nor, even when it comes to confusion, it does not forbid all possibility of confusion, nor does it elevate the interest of the easily fooled — there must be a likelihood of confusion and that must be among an appreciable segment of reasonable consumers. See Missing the Mark *supra* note 16 at ___. In contrast to some of the harsher results of the current approaches, the new factor encourages a measured response to cyberspace interventions. It expands the net for cyberspace interventions but couples this with a narrowed and proportionate remedy.
would remain in any one role to the exclusion of others, the focal point offense and
the new factor provide meaningful tools to consider what cyberspace is, what
values it has, how its values affect a public interest, what exactly happens there,
and who the characteristic users were in any mark–type conflict.

Most importantly, the focal point offense and the new factor encourage a
realistic remedy proportionate to the offending use. The remedy itself will provide
the empirical test—a disclaimer and a forced redirect in cyberspace can be
designed to be effective, at a point before the consumer has committed. If the
offending user/competitor really were providing value-adding goods or services,
the existence of the effective disclaimer and redirect will put that proposition to the
test. With an effective redirect in place, only those prospective consumers wanting
goods and services from the offending user would choose to see them. All others
would be sent back either to the mark proprietor or to the point at which they
desired to resume their search. There may be marginal frustration to some of the
factional interests in cyberspace, but not much, and much less than already exists.
But the reward will be to support the inherent capacities of cyberspace. The focal
point offense and the new factor directly support both the foundational values
(access, navigation, information, augmentation and trust) and the commercial
architecture (including authentication in the broadest sense) of cyberspace. The
focal point offense and the new factor certainly appear to work from the market
cost perspective. It seems highly probable from the normative and predictive
aspect that the proposed solution will be at least Kaldor–Hicks efficient, if not
Pareto efficient as well. Moreover, it is not as if the costs of the proposed
solution are being compared to some ideal situation, or even to a flawed but
workable situation. There is no other competing solution, and the current chaotic
situation is so far from workable it would be hard for the new factor not to improve
upon it.

7. Pirates, Plagiarists and Third Parties Who Might be Secondarily Liable.

Some of the previously named actors are pirates or plagiarists. Others are
special targets for secondary liability, targeted by opportunistic plaintiffs seeking
to lay off their costs of policing. Yet others are unexpected victims. The focal point
offense offers a ready rule of thumb for distinguishing one from the other. It also
solves the problem of potentially outlandish secondary liability arising from new
technological uses in the code world.

B. New Institutional Economics: Accounting for Juridical Agency Costs

No account of costs can be complete unless the costs are fully distributed. Not
only are there primary users who are directly burdened by mark-type conflicts in
cyberspace (the surfers, mappers, spoofers, trappers, spoilers, arbitrageurs, shills,
advertisers, shoppers, searchers, consumers, competitors and mark proprietors) but

---

308 Pareto optimal signifies a reallocation in which at least one person is better off, and no one is worse
off; Kaldor–Hicks optimal signifies a reallocation in which at least one person is better off, and though another
person may be worse off, the aggregate benefit exceeds the aggregate loss. See [pick one].

309 See Non-Neutral Principles, supra note 18 at __ and note [172] (enumerating some of those); and see
supra section II, resolving the burden of excessive secondary liability, including by way of shared responsibility
for the cost of reasonable technological accommodations.
there are transaction costs that must be absorbed by a second affected group. Let us refer to this second group as “juridical actors.” These would include judges and their clerks, professors and their students (and others who are in the business of explaining the ways of the law), and practicing lawyers and their clients. Each of them bears a cost. Because each has finite time and capacity to spend on the problems of marks in space, each is constrained in some sense and the impact on each of these actors ought to be considered when estimating the full cost (and benefits) of a new proposal.

1. Lawyers and Their Clients

   **Clients.** By “client” I mean not simply persons generally interested in a rule of law, but the subset who realize they may be particularly at risk of being made to answer for their conduct before a court of law (or who may receive letters advising them of that possibility unless they amend their conduct). The term refers to those consumers of the rule of law who visit lawyers either for counseling prior to acting, or for help after being alerted to a problem. Like the other juridical actors, clients are constrained from solving the problems.

   Clients who face juridical risk are competitively constrained from creating a “better” rule for trademarks in cyberspace. Some clients are owners of trademarks and thus are protectors of their own rights. Others are alleged offenders against rights asserted against them. The same client, and perhaps most clients who are invested in trademarks, is sometimes the accuser and sometimes the accused in respect of allegations of trademark infringement. Because there is no “plaintiff’s” bar or “defendant’s” bar, but a combined group, many clients might prefer a balanced approach (neither overly expansive nor too relaxed). Clients, however, find that the dynamics of competition in the face of uncertain and unpredictable juridical risk tend to push towards a more expansive reading of trademark rights in cyberspace. Among the ordinary reasons for pressing a claim is the fear that by not doing so, a client will be left behind or defeated by others pressing a more extreme position. Thus, while a client might prefer a moderate approach, their trade association, interest groups, and sometimes their own counsel often urge a more extreme bias. The new factor creates the safest of safe harbors. It sets practical limits, tuned to the real issues and sensible to those trying to test those limits as well as to those simply wanting to know what the limits are in order to calculate the cost of a business plan or project implicating marks in cyberspace. The “cost” would be the loss of a roulette wheel type of payoff calculation, but the benefit would be the substitution of a more certain, less risky, calculated return.

   **Lawyers.** Practicing lawyers might be the best audience for entertaining a new approach. Some of them may be circumstantially constrained from finding the “better” solution because they believe they have already heard it all and are in too much of a hurry to evaluate a new idea, and they know the dynamic constraints of competitive lawyering in the face of juridical risk. But if something really works, practicing lawyers may well be the first to notice. A specific program might establish and embrace a code of normative conduct.\(^{310}\) The focal point offense and

\(^{310}\) Groups including, but not limited to, the International Trademark Association, the American Intellectual Property Law Association, or the American Bar Association Section on Intellectual Property Law
the new likelihood of confusion factor not only establish concrete factors to assess the risk of liability, but their shared common remedy sets both a presumptive floor and ceiling on the cost of non-compliance. When it is known that a cyberspace intervention (focal point offense) may result in one or more of a technologically effective (a) disclaimer, (b) notice, (c) forced release/redirect, (d) reciprocal auction/reassignment or (e) opt-out, then effective business planning may take place, fruitful negotiations between parties may occur, and the constraints of norms, markets, code and legal regulation may begin more nearly to coincide.

2. Judges and Their Law Clerks

Notwithstanding carefully crafted opinions, judges are systemically constrained from finding the “better” rule in hard cases involving the intersection of technology and trademark law. They haven’t the time or the technical expertise to become savvy with cyberspace, the new machines on display there, or the new mark-type conflicts or underlying economics characteristic of cyberspace. The same applies to their clerks, though perhaps the clerk might be more of a hobbyist or hanger-on in cyberspace. This is as New Institutional Economics would have predicted and is a matter of observation as well as prediction. Judges are good at exercising judgment, and are very good at reading legal materials. Their clerks are trained in reading appellate decisions, and become very good at helping their judges to write opinions. Neither is generally recruited for their skill at engineering or talent in the metaphysics of intellectual property, nor would it make sense for them to be so trained or selected.311

We are looking for a new heuristic, or rule of thumb, by which these cases might be more efficiently decided. The focal point offense and the new factor provide just such a solution. It is true beyond dispute that under principles of ordinary trademark law as developed in ordinary space, mark-type conflicts hinge upon likelihood of confusion, and that likelihood of confusion is a fact-based inquiry. It is one of the most fact-based anywhere in the law. It famously requires a weighing of factors of indeterminate weight, an exercise in “effing” the ineffable.312

Well, then, what exactly counts as a relevant “factor” to “weigh” in cyberspace mark-type disputes according to the traditional tests currently employed? The cases are surprisingly and embarrassingly devoid of useful or relevant facts, and there seems to be no available evidence that would fill the existing void at any reasonable cost. The new proposal arms judges with something useful. The factual questions for the focal point offense include these: is there tampering, spoofing, ambushing, or spoilage and waste? The factual headings under which the fully specified likelihood of confusion factor will focus an intelligible factual inquiry might take the lead in recommending or publicizing professional norms.

311 See supra note ___ (discussing systemic judicial risk and citing to Professor Bainbridge’s intriguing work). It should go without saying that this is no criticism, much less an indictment. It would violate common sense were it otherwise. Judges ought to do what they do best, which is to apply judgment. Electrical engineers and network topologists ought to design new machines for new technological uses. What is needed is an appropriate mediating heuristic rule of thumb to enable judges to decide, and to instruct juries on how to find evidence relating to, mark-related cases in cyberspace. I claim to have provided such a rule of thumb.

312 DOUGLAS ADAMS, supra note ___. 
include these: (a) the nature of the cyberspace intervention, (b) the nature of the offending party, (c) the nature of the supposed victim, (d) the place of use and the degree it implicates foundational cyberspace values, (e) the presence or absence of any other “ordinary” trademark factor or related factors from cognate laws, or of tampering, spoofing, ambushing, or spoiling, and (f) the presence or absence of real-time polling and any other relevant circumstances. In all cases, there is a specific common good, or public policy, in favor of access, navigation, information-activity, and trustworthy augmented presences. There is, as well, a clearly limited and proportionate common remedy.

These are something a judge and a judge’s clerk can work with, and against which there is a reasonable likelihood of assessing whether litigants have produced forensic evidence actually probative of something relevant to some rational inquiry. It would be a great improvement over the ritualistic incantation of “just so” speculation attached to the more general factor lists (according to the current general factor lists, one would need a plausible answer to the question: is the cyberspace intervention addressed to a set of consumers who are “sophisticated” or not? Who on earth knows, and what possible evidence can be produced to attempt a meaningful answer?) To assert the new factor is better than current legal norms is about the same as asserting something is better than nothing.

Moreover, if there is some concern about the necessity of a court’s performing a gate-keeping function one result of the new analysis will be to prevent certain trademark infringement cases from reaching a jury and to prevent any focal point cases from resulting in excessive remedies. In the first place, the new factor provides a legal basis for rationally determining whether a plaintiff has produced a legally sufficient case of trademark infringement in respect of any invisible or attenuated use. It does not require a judge to substitute her wild guess for a jury’s wild guess. Instead, it permits a judge to rule, as a matter of law, in the event a plaintiff fails to produce evidence. In the second place, the new factor includes a limited and proportionate remedy, and hence a basis for fairly fitting the remedy to the offense. Where the facts permit a case to go to a jury and where a jury finds for the plaintiff, there is nothing requiring a disproportionate remedy. To the contrary, the new factor is designed to encourage a judge to tailor an equitable remedy precisely to fit the harm. Because damage remedies will probably remain rare, and the threat of a disabling injunction will become increasingly remote, the threat of a runaway jury or of an erring judge becomes a non-issue.

The focal point offense and the fully specified factor for assessing likelihood of confusion encourage a judge to enter flexible injunctive relief, including one or more of a technologically effective (a) disclaimer, (b) notice, (c) forced release/redirect, (d) reassignment by reciprocal auction, or (e) opt-out/opt-in. This is, of course, without prejudice to other more familiar remedies in appropriate cases. They set both a floor and ceiling for many cases of invisible, attenuated and expropriating uses of markers and spoilers in cyberspace.

The focal point offense and the new factor seem to be a net positive to judges and their clerks. The cost is limited to considering some new terminology and factors; the benefit is a more easily explained, readily applied, and fairly administered standard. Cases would move along more rapidly with less judicial
overhead. The focal point offense and the new likelihood of confusion factor seem to be efficient to learn as well as fair to apply.

3. Professors and Their Students

Law professors are accidentally constrained from proposing “better” rules in hard cases involving the intersection of technology and trademark law in cyberspace. They are for the most part without portfolio and, sometimes, without credibility not only with judges but with practicing lawyers. Though some are former engineers and some devote scholarly time to mastering the technology, many are not and many others tend to write too narrowly or too obscurely to gain traction with bench or bar. Despite the glamour of the law review piece, there are so many now published it is by no means certain even good work will come to the attention of any sufficiently significant population of the workaday world.

The focal point offense and the new factor do not prevent any professor from spinning a new theory out of nothing, nor does it prevent invention of bad poetry and ersatz policy to those who relish such. It does, however, provide opportunity for cooperative work. The focal point offense, the new factor and the new approach they take could be fertile ground for additional work. The economic arguments, for example, advanced herein lack empirical support. The analysis of the various interests involved must, necessarily, be supposed to be incomplete. Even the particular terms, terminology and proposed definitions could be improved upon. There is room for development and for improvement. The cost seems non-existent and there may be some benefit.

4. Commentators, Press, Poets and Public Support for the Rule of Law

A full account of the price of the focal point offense and the new factor must also weigh its effect on the public perception of the rule of law. There is the occasional need to explain “the law” to the public who are the law’s ultimate consumers. It is always possible to take the bleak view: the law is what it is, but no one knows why (a general felt cynicism), or the law seems bent on destroying cyberspace because of some culpable or laughable ignorance, or some ominously vague animus, bias, class or factional interest (a particular felt cynicism).

It would seem rather nice to be able to say the law is reacting to real relationships and new disputes in an objective cyberspace by defining what is happening, to whom, and where, and then by doing its best to articulate the public interest, to reflect upon how existing law might be transformed to afford a basis for supporting the public interest within a rule of law, and by emphasizing the solution is itself a reasonable technological accommodation broadly permitting free and robust access, navigation, augmentation, information-activity and trust while discouraging the opposite. The corresponding and proportionate remedy for offending cyberspace interventions (focal point offenses) does not shut down, but opens up cyberspace access and navigation. The only price for adopting the focal point offense is the loss of some measure of cynicism, but the benefit includes increased public confidence in the law’s ability, at least on occasion, to do something right, and to do it for the right reason, and to be able to give a persuasive explanation. Perhaps there is a constituency for pirates and who might
be disappointed, but when they learn that the solution is merely to require the pirates to stop tampering with directional signals and vandalizing cyberspace, but otherwise lets them engage in their occupation, maybe even they will recognize the advantages of the focal point offense and the new factor.

C. Avoiding Unbearable Costs (a Remedy in the Public Interest)

A full account of the costs and benefits of the focal point offense and the new factor must also weigh the unanticipated costs. Cyberspace is characterized by change. Legal standards tend to lag behind. By the time a problem gets to the stage of a reported appellate adjudication, or by the even later time a “rule” or response is designed for the problem, the technology has moved on. Cyberspace is also characterized, as is any technology, by unexpected connections, ripple effects and consequences. Any external pressure on a developing technology, especially a legally compelled pressure, can have substantial economic and other consequences. It seems law is ill equipped to intervene and some might say the common law is the most ill equipped of any sort of law.

Experience shows these to be serious but not insoluble concerns. Current cases in cyberspace have gloried in the minutia of obsolete methods, outdated technologies and old business plans. They have lurched from the extreme of banning just about any sort of invisible or attenuated use to the opposite of letting almost any sort of expropriating or predatory conduct go. Paradoxically, the answer is not to do nothing, but rather to do something more nearly calculated to solve the dilemma. The desired solution balances between generalities that remain banal platitudes or mere paraphrasing of the ultimate standard, and specifics too closely aimed at particular passing fads. Both the focal point offense and the new factor are designed to work at the right level of specificity. The focal point offense is specified to find and prevent tampering, spoofing, ambushing and spoilage. At the level of liability, the fully specified likelihood of confusion factor takes into account: (a) the nature of the cyberspace intervention, (b) the nature of the offending party, (c) the nature of the supposed victim, (d) the place of use and the degree it implicates foundational cyberspace values, (e) the presence or absence of any other “ordinary” trademark factor or related factors from cognate laws, or tampering, spoofing, ambushing and spoilage, and (f) the presence or absence of real-time polling and any other relevant circumstances. It is hard to imagine what factors other than these could be relevant. They are sufficiently distinct and clear so a client and counsel will be able to prove their presence or absence and the relative import of the mix.

The main concern must be the unintended juridical disaster. While current approaches seem on a collision course with chaos, the focal point offense and the new factor avoid spectacular failure. That is, they may very well (as might any rule) produce an occasional “bad” result, but it is very unlikely to produce a catastrophic failure. It is the flexible remedy which provides the backstop. The proposed common remedy for a cyberspace intervention includes one or more of a technologically effective (a) disclaimer, (b) notice, (c) forced release/redirect, (d)

313 See supra notes 98 to 101 (glossing the focal point offense).
314 See supra notes 151 to 159 (glossing the “nature and place of use” factor for likelihood of confusion).
reassignment by reciprocal auction, or (e) opt-out/opt-in. These will not cripple cyberspace. They will almost certainly improve it. The results will not change the ordinary law of trademarks by doctrinal creep or other mistaken application outside of cyberspace and so will not upset the current balance of trademark rights in ordinary space.

No approach failing to account for the potential cost of a crippling misapplication or catastrophic failure can be said to have been fully priced. This new approach is perhaps unique in its ability, not only to present an estimate of its costs and benefits, but to give them in a more nearly fully priced form.

**IV. SATISFYING THE CAPABILITY PROBLEM: IT IS AUTHORIZED**

The fourth claim is that the focal point offense and the new factor are authorized and capable of principled application. It is authorized by the logic of cyberspace, it resolves the capability problem, and it points the way for further work in the code world.

**A. The Logic of a Law for Cyberspace**

I have proposed a law suitable for an objective cyberspace. I claim it is authorized from several perspectives. *First*, it is authorized by the converging logic of laws, norms, markets and architecture. Trademark law has consistently permitted the consideration of any factor that is relevant in assessing the likelihood of confusion. The new, fully specified “nature and place of use” factor is relevant to the inquiry. Unfair competition has traditionally recognized various specified offenses that disrupt markets. The new, fully specified focal point offense is a designed response to the well-recognized abuses of focal points in an objective cyberspace. It is much like a tort. In fact, it is. There is a certain “naturalness” about tort law—an axiomatic understanding that it is simply wrong to cause intentional harm to another, and an axiomatic understanding that a person ought so to use their own resources as to do no unnecessary harm to a protected interest of another. The maxim “*sic utere*” has served for more than a thousand years and in various legal traditions as a starting point for working out proper and, in the wider context of trademark law’s provenance, for working out fair from unfair competition. Trademark law is different from other intellectual property because it is an activity, not a thing. My proposal is consistent with the traditional understandings, merely adapting them to the reality of an objective cyberspace.

*Second*, it is authorized by the ethos and rationally desired norms of an objective cyberspace itself and by the felt needs of the code world. The functional

---

315 See supra notes 141 to 146 (glossing the common remedy).
316 [add any of the obvious references]
317 RESTATEMENT, supra note __; see trade secret, persona; and see the older cases of waste and bad faith. While I would not recommend going quite so far as some commentators, see Viva R. Moffat, Regulating Search, 22 HARV. J.L. & TECH. 475, 499 (2009) (recognizing the “good work that the federal courts have already done” in search engine disputes, and suggesting that federal courts be encouraged to apply “either state law or develop federal common law where appropriate in the interstices of already existing statutes”), it is not a very far throw to do what courts have always done with likelihood of confusion, which is to pursue all evidence relevant to the inquiry.
318 [Coke’s case, supra note __].
characteristics of access, navigation, information-activity, augmented presences and trust generate an ethos and a value system suitable for legal protection. There is a need for a limited and proportionate response to permit a robustly navigable code world that is useful for effective information activity by vulnerable augmented presences. The limited remedy is expressly designed to be woven out of the same code-capability that created the code world, without unduly limiting the freedom of access in cyberspace. Reasonable technological accommodations constitute the same material as is typical in cyberspace and are the appropriately coded response.

Third, it authorized by the law’s own developing dynamic as a command or rule that is reasonable, directed towards the common good, articulate, and legitimate. The common remedy is characterized by a reasonable technological accommodation that resolves all of the interests affected. It is not the product of any particular faction or single interest group, but is aimed at the common functionality and desirable attributes of cyberspace itself. It is readily explainable, both as an independent focal point offense, and also as a new “nature and place of use” factor for assessing likelihood of confusion. The limited remedy is authorized and the exercise of juridical regulation is certainly as authorized as any of the already existing alternatives.

Fourth, it is authorized as a deliberate choice to transform existing legal resources to meet the need to design a law that is suitable for cyberspace. Existing principles of ordinary trademark-related law simply do not work. It is now fairly well understood that there is no “everyone-is liable” style of initial interest confusion, but there are some cases in which there actually may be a genuine preclusion style of initial interest confusion. After accounting for the preclusion-style cases, there remains a large body of cases that need to be decided. In respect of that large body of cases, it should now be fairly well understood that there is no legitimate way to dismiss those cases under some blanket “no one-is liable” style of “use as” threshold. What we are left with is the set of cases in which we need to consider: if “some” are liable for “something” then what exactly, and on what basis? My solution works, the others don’t. My solution is explicitly designed to transform existing law into a law purposely fitted to the problems of invisible, attenuated and expropriating uses in cyberspace. There is no other such comprehensive and coherent solution in sight.

B. Resolving the Capability Problem

I have been concerned, not only with allocating the costs and benefits of my new proposal to the typical cyberspace actors, but with assessing the systemic capability problems faced by juridical actors. My claim is that time spent mastering a fairly straight-forward set of terms based on manifestly observable widely experienced facts about cyberspace will provide the necessary ability for a shift from techno-babble to a techno-realist jurisprudence suitable for application of ordinary judgment to ascertainable facts and real relationships in cyberspace.

It would be folly to expect lawyers, judges, juries and clients to become bad electrical engineers or network topologists, rash to entrust the determinations to the testimony of battling experts, and odd to do so against a set of existing standards
that are inapt, and liable to lead to false positives and to weak confidence inferences. The new focal point offense and the fully specified “nature and place of use” factor for assessing residual likelihood of confusion are both limited by the common remedy, and both provide a reliable rule of thumb. The new heuristic provides a method for arriving at the correct result, for the right reason, persuasively explained, while at the same time guarding against the potential for catastrophic error. It avoids the capability problem, and also the null hypothesis. That is to say if the new approach is not adopted, it is not as if the existing problems will go away, and if it should be remarked that the new approach requires some investment of time and study, it is only fair to respond that so does the existing approach—the only difference being that the new approach can actually work and existing approaches are accompanied by so many anomalies and special doctrines as are unlikely ever to work.

C. Prospectus: What Remains to be Done

Granting that influencers of conduct in the code world include laws, norms (and normal virtues and associations), markets (and economics, more generally speaking), and architecture, the question remains: “how, then, shall we chose” to design a law suitable for the code world? A first hunch is that the designed law ought to fit with the normative virtues, economics and architecture of a coded world. Here are some suggestions for further work in each area.

The norms of the code world are characteristically plastic. They change, and they are changeable. Moreover, the norms are by no means guaranteed to be beneficent, open, or free. Not unlike normal virtues in ordinary space, the normal virtues of a global/tech era in cyberspace can be enjoyed, fostered, and displayed in a place without extrinsic scarcity, and without necessary rivalry. But the virtues of cyberspace implicate a public goods problem: if others are getting away with a norm that will not or cannot prevent piratical, predatory, parasitical and free-riding vandalism, then piracy will become the norm. It takes a choice to design architecture to penalize one norm (the pirate’s norm) and to reward or incentivize another norm (the hitchhiker’s and the guide’s norm). While technology has no inherent nature, its design does have a specification and its users do have reasons to value certain uses of the technology. These create a virtue-defined norm for the code world which ought to be preferred.

The economics of the code world, at least as it relates to dynamic focal points incorporating marks, should be reconsidered. I have proposed a comprehensive solution that dramatically reevaluates and necessarily readjusts the assumptions of scarcity, rivalry and excludability of the “goods” in question. These goods are coded constructs, many of which can be multiplied in a way that would have shocked the classical, and any other sort of economist. Moreover, I have revisited the public goods assumption, and I have driven the presently artificial-contrived shortage premium down so that the price-potential of focal points more nearly approaches the cost. This drives out the opportunity for arbitrage otherwise existing in markets for dynamic focal points, including those which incorporate marks. As a result, the market (or economic) incentive for focal point abuses is very nearly eliminated. This proposed solution aligns the legal with the economic
and the normative so that the influencers all point in the same direction.

The architecture of the code world permits discrimination, polling, and reasonable technological accommodations to resolve the offensive conduct that (a) alters the virtual map, (b) plants deceptive focal points, (c) ambushes a user of focal points with uninvited or false invitations, or (d) expropriates, blocks or spoils focal points otherwise available. It is the power of the same code that created the problems also to remediate the coded problems that forms an attractive part of the common remedy. Where the architecture itself conforms to the legal, normative and market-driven influencers, this congruence helps to reinforce a robust and comprehensive solution.

My proposal is part of a new movement in the law. The law and morality movement (or the move to a normative jurisprudence in accordance with specified principles) is voluntarily constrained by the existing law as it is. It does not simply make up new law by some combination of bad poetry and ersatz policy. It proposes a specified common morality as the basis for legal rules suitable for a global.tech era. This article claims the new factor fits comfortably within the capability of juridical agents, and is a recognizable transformation of existing law capable of principled, practical and predictable application. Most significantly, this approach finally answers the question: “how to choose?” by making actually making a definite design choice in accordance with explicitly identified goals, or ends, to be attained. In one sense, the end is to discourage predators and pirates, and to encourage value added resource providers—and that is satisfied by specified rules which distinguish one from the other. In another sense, the end is merely to provide a clearly marked object so that we might know where we are trying to go so that juridical agents might figure out where they are taking us.319

Epilogue (Where’s the Dog?)

This Article began with the parable of the poisoned flowers, and the dead dog. The dead dog in cyberspace is a world away from the barking dog in ordinary space. As Professor Mankiw tells his parallel story confined to the world of ordinary space, Dick owns Spot, a barking dog whose barking disturbs Dick’s neighbor, Jane.320 Jane can “simply offer to pay Dick to get rid of the dog” and Dick “will accept the deal if the amount of money Jane offers is greater than the benefit of keeping the dog.”321 But the pricing reflects the underlying valuation of goods in a world of scarcity and uniqueness, not a coded world, and so we might suppose that if “Dick gets a $500 benefit from the dog and Jane bears an $800 cost from the barking” then “Jane can offer Dick $600 to get rid of the dog, and Dick will gladly accept.”322

Of course, if Dick valued his dog-holding benefit at $1,000 and Jane valued her peace at $800, then “Dick would turn down any offer below $1,000, while Jane would not offer any amount above $800” and so no deal would be reached. Dick would keep his barking dog, and Jane would put up with the racket, this being the

319 [reference Alice: the cat] [add the picture at the end]
320 N. GREGORY MANKIW, PRINCIPLES OF ECONOMICS 210 (4TH ED., SECOND INDIAN REPRINT 2007).
321 Id. at 211.
322 Id.
“efficient outcome” in ordinary space. A problem in ordinary space is that of externalities. As Professor Mankiw observes:

Barking dogs create a negative externality... Dog owners do not bear the full cost of the noise and, therefore, tend to take too few precautions to prevent their dogs from barking. Local governments address this problem by making it illegal to “disturb the peace.”

The contrast between the coded space and ordinary space is stark. The expedient of rewriting the code dispenses with the externalities and upsets the scarcity-imposed valuations of ordinary space. Notice that Professor Lessig—dealing with the poisonous flowers in cyberspace—need not ask whether Martha values her poisonous flowers at $500, or $1,000, or millions of dollars; nor need he ask whether Dank valued his dog at $600, or $800, or millions of dollars. In cyberspace, all we need to know (or to assume) is that the code may be rewritten at zero or negligible cost. For the equivalent of a nickel or a dime, the parties can actually dispose of what would otherwise be an expensive or frustrating conflict. Martha keeps her flowers as effectively poisonous as ever, and yet Dank keeps his dog, no longer subject to being poisoned. Neither has to pay the other to do without.

It is striking, after all the years spent pretending to “Coasian conditions” of near-zero transaction costs, actually to find a coded world hiding in plain sight and where those conditions really obtain. But, contrary to the perhaps easily misunderstood notion that “if private parties can bargain without cost over the allocation of resources, then the private market will always solve the problem of externalities and allocate resources efficiently” and the correlative notion that

---

323 Id.
324 Id. at 204. Dogs in ordinary space come with various attributes. In cyberspace, however, dogs are creatures of code. In the code world, it is fair to ask “why not just recode the dog to prevent it from barking?” Compare SILVERADO (Columbia Pictures Corp. 1985) (asking “where’s the dog?”) and `http://www.script-o-rama.com/movie_scripts/s/silverado-script-transcript-lawrence-kasdan.html` (transcribing the script); `http://www.youtube.com/watch?v=sIJUBys2Fbs` (excerpting segments of the motion picture asking about the whereabouts of the dog) (both sites last visited on August 20, 2009).

325 Id. at 210, stating what is called “the Coase theorem” and id. at 211, claiming that according to the Coase theorem, the initial distribution of rights does not matter “for the market’s ability to reach the efficient outcome.” A person untrained in economics would have supposed the initial distribution makes a substantial difference to the persons involved. In the case of Dick and Jane—supposing, as given, that Dick’s benefit is $500 and Jane’s cost is $800, and the deal reached between them is one in which Jane pays Dick $600, the existence of a law which gives Jane the legal right to peace and quiet would tend to produce the following outcome: (a) Jane pays Dick nothing, (b) Jane pays the police and the public prosecutor nothing (Jane’s pro rata share of the marginal tax burden to fund this intervention by the police, the prosecutors’ office, and the courts being assumed to carry a near-zero, or sunk cost), and (c) Dick eventually makes his dog quiet, or else Dick loses the Dog; or the following variation: (x) Jane complains to Dick, (y) Dick predicts the likely result, based upon the legal rules, and (z) Dick offers to pay Jane $900 if she will consent to his keeping his dog (not particularly likely if Dick has several other neighbors equally prone to complain)—the initial distribution of rights matters greatly to the two parties. It is the difference between Jane’s paying $600 for peace and quiet in the absence of a legally enforceable right to her peace, and her paying nothing for her peace and quiet or, under the alternative, it is the difference between her suffering from noise for nothing, or her suffering from noise accompanied by a $900 payment. See generally, R.H. COASE, THE PROBLEM OF SOCIAL COST, reprinted in THE FIRM, THE MARKET, AND THE LAW 97-104 (illustrating the effect of legal liability rules, and the effect of no legal liability rules, in the example of straying cattle damaging the neighbor’s crops), and id. at 114-33 (adding the legal transaction costs) (1960, reprinted 1990). I am not quibbling with either Professor Mankiw or Coase, but merely pointing out that in cyberspace the transaction costs really do approach zero, the starting position really does make a difference at
the starting point doesn’t matter, the starting point, and the law’s incentives do make a difference in the code world. Indeed, the outcomes in the code world seem almost exactly opposite the results in the ordinary world, as if by a mirror-image that reverses the view.

It is also striking, after all these years spent in the code world, that the law has scarcely outpaced the level of a qualified high school student. When concepts no more difficult than algorithmic thinking, abstraction, and elegance;\(^{326}\) techniques as straightforward as sequential processing, conditional execution, iteration, decomposition, and computing a result by calling a function;\(^{327}\) and patterns as clear as establishing a requirements specification, designing a solution, implementing the solution in code, testing the code (and repeating until satisfied)\(^{328}\) are the common property of school children, it is unseemly for the “law” to be so truant in its slow advance. It is time to stop feigning an antic disposition and simply to design a law for cyberspace.

**CONCLUSION**

This article claims that a focal point offense in cyberspace can be specified, and that any residual likelihood of confusion inquiry may be resolved by a new factor: “the nature and place of use.” I also claim the focal point offense and the new factor work. The focal point offense and the new factor provide a rule of thumb disposing of cases efficiently, and getting to the right result for the correct reason, persuasively applied. Prior Articles argued current approaches fail to do so. Other commentators have, perhaps inadvertently, demonstrated all other current proposals are unlikely to do so in any way practical, principled and predictable and without creating new problems of doctrinal creep, reverse doctrinal creep and special pleading for special factions in cyberspace.

I demonstrated concrete solutions to concrete cases, using a fully specified focal point offense and a new factor coupled with a graduated and proportionate remedy in the public interest, fully articulated and based on recognizable principles of trademark-related law yet solving the problems current attempts to apply ordinary law have failed to do. This is a transformed approach. It exemplifies the insight of many, including Professor Lessig, that there are choices to be made in cyberspace—the place will be regulated, and the only important question is: how, and in whose interest? This Article proposes to answer the “how” and “whose interest” question by a focal point offense and a fully specified factor, deliberately chosen to advance an explicitly identified public interest in an embodied switched network for moving information traffic where there is a public good in access, navigation, information-seeking activity, augmentation and trust.

I claim each of the persons affected by the focal point offense and the new

---

\(^{326}\) **WANDA P. DANN, STEPHEN COOPER & RANDY PAUSCH, LEARNING TO PROGRAM WITH ALICE xi** (2d ed. 2009) (Alan Kay’s introduction to a book introducing software logic design and computer programming using the “Alice” object oriented programming application created in part by Randy Pausch at Carnegie-Mellon).

\(^{327}\) Id. at 6 (chapter one).

\(^{328}\) Id. at 23-41 (chapter two). Indeed, the project of which this article is a part takes the form of such a project.
factor is fairly burdened by the costs (and benefits) it provides. This article demonstrates there are no unbearable burdens. To the contrary it reveals the costs are minimal and the benefits well in excess of them. Modestly, but of great importance, this Article shows the new approach is much less likely than any of the existing approaches and any of the competing proposals to result in unintended consequences. The focal point offense and the fully specified factor, accompanied by a flexible remedy in the public interest, are much less likely to lead to spectacular error.

Although the focal point offense and the new factor require the use of a new set of terms, it is not as though the current approaches do not. This Article treats the current approaches as a null set and directly confronts the comparative costs of the focal point offense and the new factor against the costs of the null set. In fact, it is the current null set of equivocations, innovations, recently invented or discovered ancient norms, and cobbled-together tools that create a worse than Rube Goldberg-like cacophony of terms that are by no means simple. In fact, it is the current approach that requires juridical actors to attain or pretend to a level of expertise in computer and network theory, to take seriously various passing fancies in technological implementations and trends in metaphor and science fact, fancy or science fiction that is really daunting in its complexity. If the complexity of existing approaches had any chance of leading to better, or even to coherent results, then it might be worth the candle.

But quite the opposite is true. Mastery of the new terminology of the focal point offense and the new factor proposed in this Article is a rather straightforward exercise. Some of the new uses in cyberspace are “attenuated” in the sense they do not make an immediate association, much less an affixation of a designation with goods or services, but they certainly are “uses” of a designation made by an actor in marketing a product. Some of the new uses are “invisible” to the ordinary human observer but quite “visible” to “agents” embodied in software that prowls the net and reacts to such uses, and they certainly constitute “uses” of a designation by an actor in marketing goods or services that may cause a likelihood of confusion as to source, sponsorship or affiliation. Some of the new uses are “expropriating” because they prevent, in a way largely unprecedented in U.S. trademark law, a mark proprietor from exploiting its own mark and they divest the mark proprietor of its own goodwill. These are “uses” of a “marker” as address, magnet and/or mark in cyberspace; and they are “uses” of a “spoiler” as a roadblock or detour and/or mark in cyberspace. To be sure, these are not the ordinary use of an expression “as” a proprietor might establish a mark in ordinary space and, of course, some allowances must be made. The focal point offense and the fully specified new factor are designed to do just that. They make allowances by way of their flexible remedy, in light of factors everyone already knows are occurring. They give a name to the already-existing phenomena, thereby permitting and facilitating a designed solution.

In conclusion, the invisible, attenuated and expropriating uses of a marker or spoiler as an address, magnet and/or mark in cyberspace, or as a roadblock or detour are the paradigmatic problems of trademark-related law in cyberspace. This Article has demonstrated that the focal point offense and the fully specified new
factor: “the nature and place of use” are suitable for immediate implementation. They work because they solve real cases in a way that is practical, predictable and principled. They reach the right result for the correct reason, persuasively explained. Their costs and benefits make sense because the focal point offense and the new factor allocate them fairly among the primary cyberspace actors. It is within the reach of juridical actors and avoids the capability problems that have prevented a solution so far.

The focal point offense and the new factor ought to be embraced as the solution to invisible, attenuated or expropriating uses in cyberspace. This Article has demonstrated that the focal point offense and the new factor have three characteristics making them well worth adopting by common law courts and by practicing lawyers. They work. They are economically efficient. They are consistent with recognizable principles of existing law. They constitute a designed solution, exemplifying how code in cyberspace may be rewritten to resolve a real problem in an optimal way. They make a choice about what cyberspace may be.
APPENDIX A: THE FULLY SPECIFIED FACTOR

This Appendix is provided for the convenience of the reader, and is made available for adoption and use.\footnote{This Appendix is © Thomas C. Folsom, 2008, 2009, 2010. Permission is granted to reprint and distribute this Appendix, in its entirety or in part, with attribution and with this footnote. See Creative Commons Attribution License 2.5, http://creativecommons.org/licenses/by/2.5 (last visited June 15, 2007). A version of this Appendix has been published in [to be completed when this article is committed].} It complements similar appendices attached to my prior Articles. The reader will note that this appendix not only summarizes, but formulates the argument in rule-specific form. With suitable changes, this appendix may be converted into the form of a common law rule, a statute, or a semi-privately imposed contractual standard in the style of the ICANN-sponsored UDRP terms.

[Note: double-check, conform, and revise] [and say that other terms used without definition here are defined in Appendix B and in the text (cross reference)]

1. Definitions

(a) An objective cyberspace: an embodied, coded, switched network for moving information traffic, further characterized by varying degrees of access, navigation, information-activity, augmented presences and trust.

(b) Focal points; dynamic focal points. A “focal point” is a belief about behavior that has some kind of psychological salience, often used in game theory to explain some game-optimal solutions, especially equilibrium points. A dynamic focal point is a focal point in an objective cyberspace or elsewhere in the code world that can actually change a user’s, or a machine’s objective relationships; it can function as marker or spoiler, address, magnet, roadblock or detour; it can deliver or draw a person’s augmented presence to a location or can block or hinder a person’s augmented presence from reaching a location.

(c) New technological uses (trademark “use” of invisible and attenuated expressions). Any new technological use of a trademarked expression in a manner that may be perceived, reproduced or communicated, directly or indirectly by way of a machine or other device, now known or hereafter developed is not only subject to the focal point analysis but is also a “use” within the domain of potentially offensive conduct which might cause a likelihood of confusion of source, sponsorship or affiliation if in connection with marketing goods or services in commerce. A new technological use includes any conduct by an actor in connection with any coded expression in cyberspace and does not require any advertising, promotion or association that is visible to any human, nor does it require any conduct that would have sufficed to create trademark rights in the actor.

(d) The common remedy (reasonable technological accommodations in respect of new technological uses) [see Appendix B, glossary]

2. Prohibited Focal Point Offenses. In an objective cyberspace which relies
upon a virtual map featuring dynamic focal points functioning as markers and spoilers (addresses, magnets, roadblocks or detours), any conduct which
(a) alters the map ("tampers"),
(b) plants deceptive focal points ("spoofs"),
(c) ensnares a user of focal points with uninvited or false invitations ("ambushes"), or
(d) expropriates, blocks or wastes focal points otherwise available ("spoils"),
constitutes a prohibited focal point offense, subject to the limited common remedy. The focal point offense may be asserted by the representative of any person, place, or community of interest associated with a focal point, and who fairly represents the interested class; and it may be asserted by a resource provider which relies upon the integrity of focal points.

3. Trademark Infringement—Likelihood of Confusion for Invisible and Attenuated Expressions. Whether an actor’s use of a designation by an invisible or attenuated new technological use causes a likelihood of confusion with the mark of another is determined by considering all of the relevant factors, including:
(a) the nature of the cyberspace intervention, including the nature of the offending party and the nature of the supposed victim,
(b) the place of use and degree it implicates foundational cyberspace values,
(c) the presence or absence of any other relevant “ordinary” trademark likelihood of confusion factor or related factors from cognate laws or authoritative norms,
(d) the presence or absence of real-time sampling (or polling) and any other relevant circumstances including tampering, spoofing, ambushing, or spoiling, and
(e) an explicit assessment of the public interest in a robust and freely navigable cyberspace both at the liability stage and at the limited common remedy stage.
Unless accompanied by other circumstances, an invisible or attenuated likelihood of confusion in cyberspace is subject only to the limited common remedy, and not to the ordinary battery of trademark infringement remedies.
APPENDIX B: CYBERSPACE GLOSSARY

[Note: double-check, revise, conform and update]

This Appendix is provided for the convenience of the reader, and is made available for adoption and use.330 The following terms are among those used in this Article in a specialized manner. While they are not inconsistent with standard terminology, they are in some sense coined herein:

1. Attenuated, invisible, or expropriating [focal point or] trademark-type uses in cyberspace — uses of a [focal point] designation by an actor [and including those] which [incorporate] [fix next word] include a trademarked term of another, and which serve as invisible or attenuated address or magnet to draw users or electronic agents to the actor rather than to the other (a “marker”), or which operate as a roadblock or detour effectively expropriating and preventing another from employing its own marks (a “spoiler”). Such invisible, attenuated, or expropriating addresses, magnets, roadblocks, and detours function as [focal point] markers or spoilers rather than, or in addition to, serving “as” a mark on the Internet or elsewhere in cyberspace. Invisible and attenuated markers are said to be invisible and attenuated relative to an ordinary observer (they are [or may be focal point] markers not necessarily promoted or associated with goods or services in a way immediately visible to an observer), even though they are embodied in a tangible medium of expression from which they can be perceived, reproduced, or communicated, including by way of a machine or other device.

2. Common remedy for invisible, attenuated, or expropriating [focal point] uses — one or more of the following: a technologically effective (1) disclaimer, (2) notice, (3) forced redirect/release, (4) assignment or forced auction, or (5) an opt-out. The common remedy is additive to other “ordinary” remedies: if the only harm is an attenuated or invisible use by a cyberspace [focal point] intervention, then some aspect of the common remedy is the presumptive limit. If there is additional harm, including ordinary, visible, and direct use of an offending expression “as” a mark or otherwise causing an “ordinary” likelihood of confusion, then the ordinary trademark remedies may be added on top of these. (In the following discussion, it is assumed that Y is the intended destination, but a user is drawn to X instead because of a cyberspace intervention).

(1) A “disclaimer” in cyberspace is, by a technological means, the intervention of a non-avoidable and conspicuous message to this effect: “X is not affiliated with, sponsored by, licensed by, or endorsed by Y.”

(2) A “notice” of another address in cyberspace is, by a technological means, the intervention of a non-avoidable message coupled with a forced user-choice to this effect: “you have reached X but you might have intended to reach Y. You may reach Y [by clicking here] [by dialing this phone number].” If the offending actor is a search engine, a directory, keyword advertiser, or the like, the notice might take the form: “you have entered (or triggered an ad based on) Y, which is a trademarked expression. If you want to continue your

330 This Appendix is © Thomas C. Folsom, 2008, 2009 & 2010. Permission is granted to reprint and distribute this Appendix, in its entirety or in part, with attribution and with this footnote. See Creative Commons Attribution License 2.5, http://creativecommons.org/licenses/by/2.5 (last visited June 15, 2007). A version of this Appendix has been published in [__].
search by finding the owner of the trademark, click [here]; if you want to continue with a more generalized search for goods or services more or less like Y-brand products, click [here].”

(3) A “forced redirect/release” has two aspects, related to each other but different in their scope and effect:

(a) 3.1. A “forced redirect” in cyberspace is, by a technological means, a non-avoidable, forced change of the user’s augmented presence to this effect: the user is actually rerouted from X to Y, or the user is confronted with a required choice so the user must affirmatively choose either X or Y (and though the user is “at” X, the user cannot proceed any further in either X or Y until the user elects one or the other). If the offending actor is a search engine, a directory, keyword advertiser, or the like, the forced redirect would force an affirmative election after the corresponding notice.

(b) 3.2. A “forced release” in cyberspace is to this effect: by a technological means, the user is given instructions about how to reach Y and then is actually dropped from X altogether with instructions to try again to reach either X or Y (and the user will also have been given instructions that if the user really intends to find X, the user must enter a new “clean” address for X that really has nothing at all to do with Y, and that only the use of the clean address will actually get the user back to X).

(4) An “assignment or auction” in cyberspace is to this effect: Y becomes the owner of the offending invisible, attenuated, or expropriated marker, or else X is forced to auction the marker to a population of non-piratical users (perhaps including not only Y but also Z, another valid trademark proprietor). A reciprocal auction might require the “winner” (as well as the losers) to include mutual redirects to each other’s locations in cyberspace.

(5) An “opt-out” in cyberspace is a notice to this effect: “You are experiencing some invasive technology that intercepts your keystrokes and sends you information as a result. While some persons might consider this a feature, others might object. If you object, you may ‘opt-out’ by [clicking here].”

The disclaimer is pure information about X’s “non” relationship with Y. The notice contains information about, and a realistic opportunity to find Y (but the user remains “at” X). The forced redirect/release actually deposits the user “at” Y, or at least disconnects the user from X. The assignment/auction goes so far as to put the marker into the hands of Y (or another non-piratical user).

X. The Code World. The coded domain; an embodied, coded switched network for moving information traffic, and including as “places” within it: (1) the “metaverse” as that place within the code world characterized by the consensual association of like-minded persons (communities of interest); (2) “virtual worlds” as those places within the metaverse’s communities of interests, further characterized by a special purpose to participate, almost as citizens in what is
almost a polity subject to what is almost a social compact or game; (3) “cypherspace” (or cipherspace) as that place within the code world characterized by a need for trusted, secure and strong encryption, signature authentication, and verified message content for funds transfers, private, secure or secret communications and like activities; (4) the “blogosphere” as that place including the new “press” (where the press is not limited to a newspaper or other traditional distribution channel or medium, but is recognized as any recorded or encrypted means of carrying political speech or current history), (5) “psiberspace” (or psyberspace) as the human/machine frontier, and (6) “cyberspace” (or cyberspace proper) as that place within the code world further characterized by access, navigation, information-activity, augmented presences and trust.

3. Cyberspace — an embodied switched network for moving information traffic (a cyberspace “gateway” or an architecture), further characterized by varying degrees of access, navigation, information-activity, augmentation, and trust on the network (a foundational “activity set”). High (or deep) space displays a higher degree of these foundational characteristics than low (or shallow) cyberspace: an operational definition. Compare “shmyberspace” as a rough synonym for low or shallow cyberspace, and contrast “the metaverse” as a term that signifies a virtual reality, shared imagination, or a consensual hallucination.

4. Cyberspace Activity Set — varying degrees of access, navigation, information-activity, augmentation, and trust. The activity set is one part of the operational definition of cyberspace.

5. Cyberspace Gateway; Gateway — an embodied switched network for moving information traffic: the threshold of cyberspace, and part of its architecture. Examples include the Internet and the phone system. The gateway is a necessary, but not a sufficient condition for cyberspace: it is one part of the operational definition of cyberspace.

6. Cyberspace Interventions — consented or unconsented, harmless or predatory, value-adding or free-riding activities by an actor in cyberspace that have an objective effect on other persons or electronic agents, especially by drawing other persons or agents to a destination; by inviting or influencing other persons or agents (including directories or search engines) to list a destination as something different from or more relevant than what it is; or by preventing ready navigation to an otherwise intended destination. Cyberspace interventions are usually described from the point of view of the other person or persons affected (see “offending use”).

7. Cyberspace Resource Provider — anyone who provides essential, useful, or value-added resources in support of high cyberspace values, but especially those not conventionally rewarded for doing so: the search engine or directory provider (or any comparable service provider in respect of later-developed methods). In some cases, the search engine provider’s economic return is in contrast to that of the commercial hardware or software developer under existing conventions by which hardware and software developers routinely sell or license their products to end users, but according to which the end user regards the browser or the search engine as something that ought to be “free,” or in which some market, mechanism,
or practical factor drives the browser, the search engine, or directory provider’s price towards zero while the costs might be significantly higher than zero. There may also be significant barriers to entry for new cyberspace resource providers, especially those who must compete against providers who are government funded or subsidized, or who have dominant positions in other markets that support their resource-providing activities, or who have become previously entrenched.

8. Cyberspace’s Typical Actors (in the context of trademark-related disputes) — surfers and mappers, spoofers and trappers, spoilers and arbitrageurs, shills and advertisers, shoppers, consumers, competitors, and mark proprietors. If the public interest in trademark law generally (and in ordinary space) is already balanced among consumers, competitors, and mark proprietors, then the aggregate balance in cyberspace should not only preserve the preexisting balance but also, other things being equal, favor mark proprietors, surfers, shoppers, and mappers over spoofers, trappers, spoilers, shills, and expropriating users. The public’s interest in the activities of various economic rent-seeking arbitrageurs, including information brokers and aggregators, will vary according to the specific conduct involved.

9. Cyberspace Users (supposed victims) — a subset of the typical actors in cyberspace. Of the larger group of typical actors, it is surfers, shoppers, and consumers of varying levels of expertise and awareness who will generally be the focus of concern because these will be the supposed victims of likelihood of confusion. The same user might simultaneously act in more than one capacity and on more than one level of expertise or awareness, or a user might sequentially move from one capacity or level to another (the term includes electronic agents). In the context of expropriating use, spoilage, or waste of a mark or its goodwill, the cyberspace user also includes the mark proprietor, or the creator of the goodwill, and the actor who has expropriated the goodwill of the mark.

10. Gateway — see “cyberspace” and “cyberspace gateway” above.


12. Hitchhiker’s Guide (or “Guide”) — (1) a mapper, or a guide; anyone who places or controls the placement or allocation of addresses or magnets, publishes addresses or magnets, or otherwise promotes navigation in cyberspace by methods now known or hereafter developed; (2) a map, guidebook, or comparable resource. Something produced by a mapper or a guide, as for example, a search engine or directory; a short-hand name to describe a navigational resource provided by a cyberspace resource provider.

13. Markers or spoilers in cyberspace — expressions placed in cyberspace and that function as address, magnet, and/or mark to draw a user to an expected destination (a “marker”), and sometimes as roadblock or detour to deceive or to hinder a user from reaching an otherwise expected destination, or to prevent a mark proprietor from employing its own marks as addresses (a “spoiler”).

14. Offending Use — conduct that causes a likelihood of confusion or other specific harm in connection with marketing of goods or services. In cyberspace, an offending use includes:

[Alt. 1]. Use of an expression as an address, magnet, or mark that causes a likelihood of confusion in connection with marketing goods or services; or as a
roadblock or detour in connection with, or as an interference with, marketing goods or services that either causes a likelihood of confusion or spoils, wastes, blocks, or expropriates the value of a mark of another (see “cyberspace interventions” for an alternate formulation: offending “use” consists in any cyberspace intervention that causes one of the specified harms).

[Alt. 2]. Any conduct which causes an expression (1) to be perceived or communicated, or fixed in a tangible medium of expression from which it may be perceived, reproduced, communicated, or inserted, either directly or with the aid of a machine or device, (2) by or to any person, machine, device, or agent, including an electronic or technologically-based agent, now known or later developed (3) in connection with marketing goods or services, and (4) which causes a likelihood of confusion; or which draws, pulls, or diverts another person or virtual agent away from an intended location; or which spoils, wastes, blocks, or expropriates the mark of another; or by which marketing messages based upon a senior mark might be intercepted, diverted, or blocked.

15. Pirate; Piracy — (1) a person who commits piracy, but in cyberspace especially, one who does so by changing the map, moving markers, placing false markers, and otherwise planting deceptive magnets or addresses; or by spoiling, wasting, or expropriating markers; (2) the act or actions of a pirate: activities that tamper with the map to cyberspace or with the useful navigation of cyberspace, as by tampering with addresses or magnets or planting deceptive addresses or magnets, blocking or spoiling addresses otherwise available. A magnet or address is deceptive to the extent it draws a user to an otherwise unintended destination, or hinders a user from reaching an intended destination. Piracy is the more harmful to the extent it is the more uninvited, unexpected, predatory, and non-value-adding.

16. Polling — (1) an inquiry made to the user (potential consumer) at the point of the cyberspace intervention or within a reasonable proximity to the intervention and which seeks to determine whether the user is likely to be confused by the intervention; (2) an inquiry made by or on behalf of a mark proprietor to an offending actor which seeks to determine whether the actor is a value-added provider. Polling will typically be in relation to the common remedy—a user may be polled, and an offending actor may be polled separately: in the one case, by asking the user to select one of the remedies offered, and in the other case, by asking the offending actor to provide one or more of the notice, disclaimer, redirect/release, or opt-out procedures, thereby satisfying the user and the mark proprietor, and categorizing the offending actor at the time and place of the request.

17. Principles of trademark law especially relevant in space — There are seven principles of ordinary trademark law especially relevant to mark-type disputes in cyberspace. Likelihood of confusion (1) does not prohibit mere inconvenience or possibility of confusion, (2) can involve sponsorship as well as source, (3) is not for the small number of confused consumers, (4) raises questions of fact, (5) to the extent it is a mixed question of law and fact, must guard against errors introduced by doctrinal creep, reverse doctrinal creep, and feedback loops, (6) may be resolved at the remedy stage by flexible relief, and (7) to the extent it
depends upon a legal determination of “use,” must guard against the multiple ambiguity of “use” in trademark law, and must focus on the question whether the conduct in question is an “offending use” (and not upon the irrelevant question whether it is a “use sufficient to create trademark rights” or “use in interstate commerce sufficient to sustain federal jurisdiction under the Lanham Act”).

18. Principles of trademark-related law especially relevant to marks in space — There are other domains, outside of ordinary trademark law, that are especially relevant to mark-type disputes in cyberspace: (1) dilution, under the Federal Trademark Dilution Act or the Trademark Dilution Revision Act, (2) cybersquatting offenses, under the Anti-Cybersquatting Consumer Protection Act, (3) compelled dispute resolution, under the Uniform Dispute Resolution Policy of compliant domain name registries, (4) unfair competition offenses, under common law protection against appropriation of intangible trade values and under the Lanham Act, and (5) various norms, architectural, and market factors.

19. Use — see “offending use” and “cyberspace interventions.”