Finding Superman in Cyberspace (Poisoned Flowers, Pt. 1):
Resolving Focal Point and Trademark Disputes on the
Internet and in Cyberspace 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.1

* * *

Superman: “I . . . I thought I was the only man who could fly!”

Stranger: “But I am no ordinary man. I am Mr. Mxyzptlk!”2

ABSTRACT

In cyberspace, dynamically coded focal points (some but not all of
which include trademarked expressions) 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


** Professor, Regent University School of Law; J.D., Georgetown University Law Center; B.S., United
States Air Force Academy. This manuscript has been long in the making. I thank the International Trademark
Association (INTA), and especially Jeremy Phillips, moderator of the INTA panel in Seattle (annual meeting,
May, 2009); the Intellectual Property Scholars Conference at the Cardozo Law School (August, 2009); Baylor
University Law School and Dean Toben and Professors Swenson, Osler and Powell (guest lecture, October,
2009); and the Association of Law, Property and Society for its Conference at the Georgetown University Law
Center (annual conference, March 2010). I am also grateful to INTA for awarding me the 2009 Ladas Memorial
Award 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 begun there. My Research Assistants have included
Shannon Brown, Nathan Hall, Joanne Kelvington, Nicholas Lepire, Jonathan McDowell, Robert Noote, Andrew
Page, Benjamin Wigger, Patrick McKay, Kathleen Hodge, Wayne Wallace and Jillian Barajas. I also thank each
of the various conference attendees who graciously offered criticism and suggestions and thereby gave me the
opportunity to extend, clarify and revise my prior remarks. Among many others, these include Professors
Christine Haight Farley, Laura Heymann, Michael Landau, Jacqueline Lipton, and Alina Ng. An unidentified
audience member characterized a prior short-form presentation of these materials as being “like Lessig on
speed,” from which I took encouragement to grind out the last revisions to the increasingly bulky manuscript
(now bifurcated into two pieces). There are others, too numerous to mention by name in this opening footnote.
The errors are mine. The split infinitives are my editors’. The bulk of the research was current as of Winter–
Spring 2010 with some updating since then.


2. Jerry Siegel & Joe Shuster, Introducing the Mysterious Mr. Mxyzptlk, 1 SUPERMAN, NO. 30 (1944).
See infra Appendix A for pictures, pronunciations, variant spellings, a succinct explanation of the reference,
and its connection to “free-riding on the free-rider,” which is one effect of my proposed solution.
space is useful. Indexing them is even better. Both these activities support the public good by providing a virtual map to cyberspace, thereby promoting access, navigation, information-activity, and trust among vulnerable augmented presences (the capacities of persons perceived within, and perceiving, an objective cyberspace, but without the full sensory and other anchors provided in ordinary space). In an objective cyberspace that relies on a virtual map featuring dynamically coded focal points functioning as markers and spoilers, addresses, magnets, roadblocks, or detours, there is an opportunity to describe norms, to distinguish forms of offensive conduct in respect of new technological uses beyond trademark, and to prescribe effective, modest, and technologically reasonable remedies. I propose that conduct which: (a) alters the virtual map, (b) plants deceptive focal points, (c) ambushes a user of focal points with uninvited, invasive, or false invitations, or (d) expropriates, blocks, or spoils focal points otherwise available should be an actionable focal point offense.

All focal point offenses involve expressions functioning as “markers” or “spoilers” in cyberspace. Some of the more effective focal points incorporate trademarked expressions. Quite apart from trademark-related law, I claim the specified focal point offense in cyberspace constitutes independently actionable misrepresentation or fraud, misappropriation or theft, spoilage or unfair competition (and, in some cases, unjust enrichment). 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.

“Ordinary” 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 threatening to deface trademark law itself. Current trademark likelihood of confusion factors, even when carefully applied, cannot reliably predict a likelihood of confusion by “invisible” or “attenuated” uses of expressions in cyberspace that incorporate trademarked terms, much less resolve the real problems caused by focal point offenses. In a prior article, Space Pirates in Cyberspace, I proposed the first half of a comprehensive solution: a modified set of trademark likelihood-of-confusion factors for such cases. Now I propose the focal point offense as the other half of the solution and I explicitly link the trademark-style and focal point-style offenses into one unified theory.

The unified theory is recognizably derived from existing patterns of law already regulating misrepresentation, misappropriation, and unfair competition, and can easily coexist with current trademark-related law. Not only is it better than any other competing explanation of, or proposal for, how to deal with invisible or attenuated trademark conflicts in cyberspace, but it is the first theory ever to consider the problem of dynamic focal points in cyberspace. Moreover, it is available for immediate implementation because it is practical, principled, and predictable. It works, it is efficient, and it is authorized.

TABLE OF CONTENTS

I. INTRODUCTION ............................................................................................ 203

II. THE PROBLEM: NEW TECHNOLOGICAL USES IN A CODED WORLD .......... 206
   A. The Nature of Use.................................................................................... 208
      1. Poisoned Flowers............................................................................. 208
      2. Magic Words and Magic Horses...................................................... 209
      3. Superman Meets Mr. Mxyzptlk....................................................... 213
      4. Invisible and Attenuated Uses of Focal Points Some of Which Contain Trademarks........................................................................ 214
         a. Markers and Spoilers. ................................................................. 215
         b. Focal Points................................................................................. 216
   B. The Place of Use...................................................................................... 221
      1. The Code World and its Places ....................................................... 221
      2. An Objective Cyberspace Within the Code World.......................... 227
      3. Advantages of the Place of Use Analysis......................................... 230
   C. Designing Law: Combining the Nature of Use and the Place of Use....231
      2. The Nature and Place of Use: Dynamic Focal Points in Cyberspace ................................................................................. 234
      3. The Technique: Designing Rules for Magic Horses....................... 236
   D. When Trademark Fails ........................................................................... 240
      1. Failed Gatekeeping Rules.............................................................. 241
      2. Failed Likelihood of Confusion Factors.......................................... 247
      3. The Real Problem—Focal Points in an Objective Cyberspace.......255

III. RESOLVING THE PROBLEMS: THE NATURE AND PLACE OF USE IN THE CODE WORLD............................................................................................................. 255
   A. The Focal Point Offense ........................................................................ 255
      1. Deliberate Misuse of Focal Points.................................................. 256
I. INTRODUCTION

This article comprises both theory and application. I am proposing a rule-generating standard and I explain both standard and rule, the general theoretical method behind the standard, and a number of very practical “black-letter” rule(s) derived from it, each part supporting the other. The theory is in Section II, the practical application is in Section III and following. After this introduction, Section II of this article describes the general problem of new technological uses in a coded world. I invoke Professor Lessig’s well-known hypothetical of the poisoned flowers that killed the neighbor’s dog (and his elegant, Pareto-optimal solution in a coded world) and my adaptation of it, by way of Superman, to the problem of navigating in cyberspace by findable markers. This leads to a discussion of the “nature and place of use” as a rule-generating principle; a heuristic rule of thumb for designing law in a coded world. I define the code world and some half-dozen places within it, each having its own characteristic nature, uses, and problems. I distinguish a first order of uses that are very nearly the same as, and merely transposed from, ordinary space; a second order of uses that are in fact fundamentally and decisively different from anything that can happen outside of fantasy in the ordinary world; and a third-order problem on the

---

4. The reader will notice that this article itself follows many of the conventions of the coded world it describes. See infra notes 115, 264, 289–292 (describing some foundational conventions of coded architecture). In particular, I appreciate I am writing to readers whose time is valuable and I do not presume any of them will read this entire article in one sitting from start to finish. Like object-oriented code, this article is modular and each module is self-contained; each section or part may be “called” independently of any other. I also embody some repetition (redundancy) as a feature, not as a bug, so that the parts (modules) will cohere even if entered by the user (reader) in an order not intended by the author (me). If the reader wants just the proposed rules, in “black-letter” form, she may turn to them, and in any order: for the rule of the new focal point offense, turn to Part III.A.2., infra; for the proposed rule on transformed “use” and “initial interest” in cyberspace, infra Part III.B.1.; for the “black letter” on transformed likelihood of confusion factors, turn to Part III.B.2., infra; and for the proposed common remedy, infra Part III.C.2. If the reader wants only theory, examples, or methodology, the reader may turn to Part II (and to II.B.1 in particular for a legally relevant definition of the code world and at least six distinct places within it), infra, or to Appendix A, infra p. 295, for a nifty picture of Superman and a brief application of the Superman example.

5. I will describe the poisoned flowers example, and the Superman example, in plenty of detail later. I do not provide a glossary or index to this article in part because of space limitations, and in part because we can do something different and maybe even better now. The coded world of cyberspace makes it relatively easy for the reader to gain access to an electronic version of this article suitable for a full-text search, without charge or subscription. A click on http://ssrn.com/author=519369 (last visited on Jan. 4, 2012) will take you to the Social Science Research Network (SSRN) and will put the full text of this and my prior articles in the hands of any interested reader so you may enter any search term you please. If a reader wants to find any of my terms more directly, or merely wants to know whether I have mentioned Justices Roberts or Scalia, Judges Easterbrook or Kozinski, Glenn Reynolds or Malcolm Reynolds, Mao Tse-tung or C.S. Lewis, or wonders whether I have cited anyone they know, or any particular case, or have said anything about Magic Horses, or Harry Potter, or Alice, or Wonderland, or Ali Baba, or ruby slippers, or the Wizard of Oz, or the Lord of the Rings, or any other topic that might be revealed by a word search (there are several other Easter eggs embedded in this article), he can jump to the spot in the readily available electronic version without the need of any intermediating index. It is a coded world, after all, and welcome to it. I will mention the SSRN link a few other times in this article for the convenience of any who may have missed this reference.
2012 / Poisoned Flowers, Part 1

periphery. This section ends by describing the systemic failure of trademark law to handle invisible and attenuated uses of trademarks in an objective code world—a failure of “ordinary” trademark law to distinguish problems of the first, second, and third orders in cyberspace.

Section III of this article resolves the problems described. I apply the new rule of thumb, “the nature and place of use,” as a technique to generate adaptable solutions relative to any particular place in the code world whenever characteristic users are acting in the unique ways that code permits. Some of those users act as predators and spoilers, others act as value-adding resource providers, and yet others simply try to use the place for the purposes for which it was designed. I demonstrate this technique by applying it. From the nature and place of use, I generate a rule-specific “focal point offense” to deal with the new problems of altering the virtual map to cyberspace, planting deceptive landmarks, ambushing a user, or expropriating or spoiling navigational markers, some of which include trademarks. Then I generate a rule-specific trademark law revised for “invisible” and “attenuated” uses that may cause a likelihood of confusion in a new technological environment when measured according to the new realities of new uses within the new place. Next I describe a number of comprehensive common elements—limited remedies comprising reasonable technological accommodations including “polling”; and controlled secondary liability—to unify the legal approach and to converge law, norms, markets, and the architecture of code in cyberspace.

In Section IV, I propose to integrate not only the focal point offense and trademark law, but also the cognates (ICANN’s UDRP, the statutory ACPA, dilution, and other cobbled-together regimes) that touch upon one or another corner of the problem of attenuated and invisible uses of focal points in an objective code world. The integration of the current crazy quilt into a comprehensive and coherent whole is an additional benefit of my approach. It is a unified theory.

Section V of this article is a brief prospectus of my forthcoming article. I claim this proposal is suitable for implementation, but I mean to subject my proposal to three other tests. First, does it work? Second, is it efficient in allocating the costs and benefits of focal points? Third, can common law judges and other juridical agents implement the focal point offense under existing laws, statutes, norms, and other governing authorities? Here, I can do no more than outline the conditions for implementation of this proposal. In the forthcoming article, I will complete my proposal by fully addressing the three tests and demonstrating that my proposal works, is efficient, and is authorized. There, I will discuss details of applying this proposal.

Section VI is an epilogue that reverts to the problem of the poisoned dog with which this article begins. Section VII is my conclusion. Appendix A is an illustrated attachment that contains a reproduction of the cover art of the comic book that introduced Mr. Mxyztplk to Superman, and ties together the example and my argument.

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 the code world including cyberspace. In my prior articles, I have claimed the preliminary task is to defend two propositions: (1) that there “is” an objective cyberspace (part of a larger “code world”) with defining characteristics suitable for positing a public interest, and (2) that this defined cyberspace 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 to explicitly reconsider remedies and principles of secondary liability as they relate to new technological uses in the code world. In short, this is a comprehensive solution to a systemic problem.

7. Each of the prior articles (and a primitive version of this one, under the working title “Poisoned Flowers in Cyberspace”) can be readily found, in full text on the Social Science Research Network (SSRN) at http://ssrn.com/author=519369 (last visited on Jan. 4, 2012) (on file with the McGeorge Law Review).
10. Folsom, Space Pirates, supra note 3.
12. I have made that demonstration. Folsom, Defining Cyberspace, supra note 8.
13. I have demonstrated this to be true, at least in the context of trademarks. See Folsom, Missing the Mark, supra note 9. One sign of a systemic problem is when two lines of cases 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.
14. I began this task by first specifying a trademark law suitable for special problems in cyberspace. See generally Folsom, Space Pirates, supra note 3 (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 I began in Defining Cyberspace and Space Pirates.
15. See generally Folsom, Embracing eBay, supra note 11.
16. See generally Folsom, Non-Neutral Principles, supra note 11.
In completing the solution to mark-type conflicts in cyberspace, I am 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 reasonable technological accommodations within their coded systems to remediate the problem, either proactively or upon request. The desired solution for cyberspace must be, and my proposal is, comprehensive because each issue connects with many others.17 In this article, I complete the full specification of the focal point offense. In the forthcoming article, foreshadowed in this one, I address three practical questions: (1) Does it work? (2) Is it efficient? and (3) Is it authorized?18 In short, I claim this is a useful solution. Not only that, I claim it ought to be implemented—immediately and before the law does any more damage to the fabric of the code world.19

II. THE PROBLEM: NEW TECHNOLOGICAL USES IN A CODED WORLD

Two hypothetical cases of poisonous flowers in cyberspace illustrate the power of code in a coded world. One involves “poisoned flowers” in the strict sense and introduces Professor Lessig’s elegant Pareto-optimal example of a coded resolution to a coded offense. The other involves Superman and introduces the “free-riding on the free rider” construct that can be accomplished by means of code in a coded world. The reason I refer to both examples as cases of

17. See infra Parts III.A. (the focal point offence), III.B. (the revised trademark factors), and III.C. (the comprehensive common elements, including a limited common remedy, and limited secondary liability). Beyond this, I integrate and unify the treatment of all offenses that arise out of an “invisible and attenuated” use of a mark containing a focal point. See infra Part IV (integrating trademark likelihood of confusion and related laws). Without these and similar connections among actionable offenses, limited remedies, and safe harbors for secondary liability, the various pieces do not work well.

18. 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 text of this article. 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).

19. Legislation, like nature, often seems to abhor a vacuum. In the absence of a solid foundation for addressing real problems in cyberspace, bad legislation (like the presently pending/tabled Stop Online Piracy Act (SOPA), H.R. 3261, 112th Cong. (2011), dealing with copyright liability, but clumsily), will be introduced, and may very well shut the door to better solutions. I claim I am providing a better plan for designing solutions in the code world, and that there is an urgent need to implement it before something worse happens.
“poisonous flowers” is that each demonstrates the concept of rewriting code to resolve coded offenses—code has the power to provide a very nearly equal and opposite counter-measure to the code-generated offense. There is not much in ordinary space that is analogous to the power of code in a coded world, hence the importance of shifting the perspective from the world of ordinary space to that of a code world at the outset.

I will then turn to the specific problem of “invisible and attenuated uses” of focal points in the code world. That is, expressions, often unseen except by machines, functioning as navigational beacons (or markers) in the code world, and including those expressions that incorporate a trademarked term. The paradigmatic cases are well known. Much more will follow, but for now, think of a telephone number mapping to a text string deceptively similar to the mnemonic “1-800-HOLIDAY” but not sponsored by Holiday Inns; the expressions “playboy” or “contacts” used on the internet as triggers to draw traffic, or to target advertising by persons not affiliated with Playboy Enterprises or with the proprietor of the registered mark, 1-800-CONTACTS (and design). You might think also of the domain name, PANAVISION.COM “warehoused” and so taken away from the mark proprietor, who must either buy back its own good will, or contrive some sort of lawsuit to retrieve the address.

Deliberate deceit, theft, unjust enrichment, 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 disingenuously as a fraudulent marker or as an expropriating spoiler. Conversely, value-adding focal point conduct in cyberspace, especially when it includes technologically reasonable accommodations to mitigate any incidental harm, should not be forbidden simply because a trademark is somehow involved. This is true even if the focal point causes 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 would not be a focal point at all.

20. See Holiday Inns, Inc. v. 800 Reservation, Inc., 86 F.3d 619, 620 (6th Cir. 1996) (involving a telephone number mapping to a mnemonic text string similar to 1-800-HOLIDAY, but leading to someone other than the proprietor of the “Holiday Inn” trademark); Playboy Enters. v. Netscape Commc’n’s Corp., 354 F.3d 1020 (9th Cir. 2004) (involving the expression “playboy” used as a trigger for targeted advertising, leading to a location not owned, sponsored by or affiliated with the proprietor of the “playboy” trademark); 1-800 Contacts, Inc. v. WhenU.com, Inc., 414 F.3d 400 (2d Cir. 2005) (involving the expression “contacts” used as a trigger, leading to a location not owned, sponsored by or affiliated with the proprietor of the “1-800 Contacts (and design)” trademark. I have analyzed these, and many other, cases in some detail in my prior articles. For present purposes it is sufficient merely to flag the occurrence of these generalized fact patterns—they collectively evidence a paradigmatic problem in cyberspace. It is the problem of dynamic markers and spoilers. I will say much more about these problems later in this article, here I am merely identifying the issue.

21. See Panavision Int’l v. Toeppen, 141 F.3d 1316 (9th Cir. 1998) (involving an attempt by a person other than the mark proprietor first to register a domain name including the “Panavision” trademark and then to sell the domain name to the mark proprietor at a price greater than the cost of obtaining the domain name registration).
I propose specific rules to distinguish piratical, predatory, and parasitical conduct on the one hand from value added resource-providing conduct on the other. This will permit the legal influencers on conduct to align with norms, markets, and architecture in a code world for the common good.

A. The Nature of Use

The coded world is like, but fundamentally different from, the world of ordinary space. The code world so routinely responds to “words” that are operative, that can, and do, change the state of a machine or of another coded construct that perhaps the wonder of this is lost. To be blunt, the ability to “speak” an expression and then to see it change the state of objective reality is nothing short of the imagined power of magic and of magic formulae. This is not Kansas anymore and this is not a pretend Dorothy clicking pretend ruby slippers to imagine her way back home. This is an operatively coded world. It routinely permits uses only found in fantasy or fiction in the world of ordinary space. It would be a good idea for law to take notice of that fact. Some stories may help to reorient the reader to the new coded problems, and easily coded solutions, to the real phenomena of poisoned flowers in an objective cyberspace and elsewhere in the code world.

1. Poisoned Flowers

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 Martha’s poisonous-flower-that-kills-the-neighbor’s-dog and then easily resolves the conflict between neighbors by a reasonable compromise.

22. LESSIG, supra note 1, passim.

23. 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, Sept. 1, 2009, http://www.popularmechanics.com/home/improvement/lawn-garden/4331026 (on file with the McGeorge Law Review) (emphasis added) (quoting poison-plant aficionado and author Amy Stewart), source suggested by Professor Glenn Reynolds, INSTAPUNDIT.COM (Sept. 18, 2009, 4:35 PM), http://pjmedia.com/instapundit/85364/ (on file with the McGeorge Law Review).

24. The hypothetical’s conflict concerns a dead dog. LESSIG, supra note 1, at 9–10. 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. Id. at 10, 12. As Professor Lessig soon reveals,
25 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. Id. at 12. 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. Id. at 13. In short order, the conflict is resolved to everyone’s satisfaction, and at essentially no cost, other than some slight 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).

26. See, e.g., id. at 85–99 (describing four things that regulate or influence conduct: laws, norms, markets, and architecture); id. 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.

27. See Frank H. Easterbrook, Cyberspace and the Law of the Horse, U. CHI. LEGAL F. 207, 208 (1996) (asserting that the law of contracts, property, or tort might be all that is necessary to understand legal relations in or affecting horses, and that copyright, patent, or other substantive law might be all that is needed to understand any law of cyberspace). Easterbrook concludes that we must “[d]evelop a sound law of intellectual property [outside of cyberspace], then apply it to computer networks.” Id. For one set of problems, he is right.

McGeorge Law Review / Vol. 43

technological accommodation: upon request and after a short conversation, Martha, the offending party, simply rewrites the code to change the properties of the poisonous flowers, and in a Pareto-superior move to boot. Let the flowers remain poisonous yet beautiful and so retain their economic value to Martha and her customers, but simply let them lose the property of being poisonous whenever any flower blows off her land and so preserve the life of neighboring dogs and small children. Of course, Professor Lessig’s story occurs in a coded world. This is a world regulated and influenced by a combination of laws, markets (prices), norms, and architecture.
In an objective code world, characterized as an embodied switched network for moving information traffic or for changing the state of a machine or another coded construct, coded utterances ("speech") become operative. I can code a flower, a dog, or a horse. When I code a horse, I not only reify it, but I can also create a class of horses sharing properties, methods, and functions. I can embody "state" in an object-member of that class and can use computation to change the state. That is to say, object-oriented code gives its author several advantages. The author may create a class, and thereafter multiply and instantiate object-members of the class, any one of which inherits all the properties, methods, and functions of the class, pretty nearly at will and without any additional marginal effort or other cost. The author may then invest any particular object-member with specially coded additional features, and may use coded methods to compute changes to the "state" of the object that will be effective to transform it, or one of its attributes, from one state to another—once I have made a class of "horses," it is easy to make any number of them and in any size, color, strength, speed, longevity, or the like, and to vary any of those attributes, and it isn’t very hard at all to put wings on some, or a single horn on others, either as special attributes within the class or as a new class of flying horses or unicorns. Because the words or other expressions of the author are actually operative upon execution (as if, were they spoken words, operative upon utterance), the effect is very much like magic. One speaks, and reality itself changes. As Professor Lessig asks, since code generates its own world according to its designed nature, "why not change the laws of nature" to eliminate the conflict between Martha and Dank?  

In at least some places in the code world there is something happening that is without any nonfantastic likeness or analogy anywhere in the world of ordinary space. There in the code world, I am not simply crying "fire" in a crowded theater. Instead I can cause the theater to burst into flames by executing a "fire" command 29 or to vaporize and disappear by uttering a "delete" command—what else am I doing when I seize control of your computer and start deleting or corrupting files? Nor are we just imagining that we might, with Ali Baba against the forty thieves, say "open sesame" and a door might open. Rather, if your password is "friend" I can actually "speak" that word and enter as a thief into

28. LESSIG, supra note 1, at 13.
29. Compare J.K. ROWLING, HARRY POTTER AND THE DEATHLY HALLOWS 59, 342 (2007) (casting a spell by uttering the expression "Confringo" thereby causing an object to explode in flames), and id. at 635 (reciting the "Fiendfyre Curse" to produce an uncontrollable fire taking the form of a beast), with J.K. ROWLING, HARRY POTTER AND THE ORDER OF THE PHOENIX 792 (2003) (describing the effect of Antonin Dolohov’s curse as creating a streak of purple flames). None of these really produce objective effects outside of the book, the movie, or the imagination.
your most private domains in the code world. In ordinary space, we might don a pair of ruby slippers, click them together and only imagine or pretend we ended up in Kansas. But if I utter “Kansas” into my browser and then click, I, or more accurately, my augmented presence will surely go somewhere that leaves an objective trace and in which I can create or change real relationships in an objective reality that can have legal as well as other practical consequences.

What we routinely call “code” in the metaverse or elsewhere in the coded world is what we would call an incantation if it actually worked in the ordinary world. Outside of the code world and apart from the speech of God, or what we would call magic or miracle if it happened in the world of ordinary space, nature is not so readily changed.

Remembering Professor Lessig’s well-known parable, Martha’s poisonous flowers can kill the neighbor’s dog when the wind blows them from Martha’s property to Dank’s. But these are poisoned flowers in a virtual world operating under its own coded architecture, and Martha may at essentially no cost to herself simply recode her flowers so they lose their poison when they leave her property without her permission, saving Dank the trouble of making yet another new dog. These are not “normal” flowers and these are not “normal” dogs, nor is this the ordinary law of nuisance or climate control nor is this the ordinary economics of scarcity and transaction costs. We ought no longer to be thinking exclusively in

31. J.R.R. TOLKIEN, THE FELLOWSHIP OF THE RING, LORD OF THE RINGS 297–300 (Houghton Mifflin 1994) (1954) (opening a gate in solid rock under the inscription “Speak friend and enter,” or “pedo mellon a minno” in the Elvish, by speaking the word “friend” and then entering the concealed caverns of Moria—an example of what we call “magic”). The word itself is operative, and its utterance changes the state of objective things.

32. THE WIZARD OF OZ (Metro-Goldwyn-Mayer 1939) (clicking her heels while repeating “there is no place like home” takes Dorothy back to Kansas); L. FRANK BAUM, THE WONDERFUL WIZARD OF OZ 258 (1900) (semble, making the slippers silver and the incantation simply “Take me home to Aunt Em!”)—but that is only a book, or a movie; it is pretend, nobody actually went anywhere.

33. Neal Stephenson, who may have invented the term “metaverse,” has one of his characters explain that “[an expression, said to be Sumerian, perhaps transliterated in a nonstandard way] is a speech with magical force. The closest English equivalent would be ‘incantation.’ . . . Nowadays, people don’t believe in these kinds of things. Except in the Metaverse, that is, where magic is possible. The Metaverse is a fictional structure made out of code. And code is just a form of speech. . . .” NEAL STEPHENSON, SNOW CRASH, 211 (1992). Of course, the objective metaverse that I describe and define for legal purposes later in this article is not itself fictional. But it is constructed of code, and the construct itself may be changed by code. It is a place where code (if not magic) is possible. We are so blinded to coded reality that we might well call it magic. I call it “operative speech”: speech that is effective upon utterance to change objective reality. In an objective code world, code is effective to move information traffic, to change the state of a machine, a living being, or other code.

34. Compare “In the beginning was the Word, and the Word was with God, and the Word was God. All things were made by him; and without him was not anything made that was made.” John 1:1–4 (King James), with JOHANN W. VON GOETHE, FAUST: THE FIRST PART, lines 1224–37 (George Madison Priest, trans. Alfred A. Knopf 1941) (1808) (describing the travail of Doctor Faust, attempting to translate the first sentence of the foregoing text in a manner that gives full effect to the power signified by it: “In the beginning was the word [no, not enough] . . . the thought! [no, not right] . . . the power! [not quite] . . . the deed!” [whereupon Faust stops, apparently content with his rendering, at least until the Devil, Mephistopheles, drops by to offer him some counterfeit power]).
terms of Judge Easterbrook’s famous metaphor of ordinary horses simply transposed into cyberspace. Some are. Others are not simply transposed but are state-shifting coded constructs (including coded horses in the code world).

These coded horses, created by will and words, reproduced and multiplied at almost no cost, distributed essentially for free, and adapted or modified as we please, have no real likeness to any similar things or to any similar powers affecting them in ordinary space. This is exactly what we would call “magic” words and magic horses if any such thing existed in the ordinary world. But it is merely what we call “code” in the code world. And it is as common there as it is utterly unprecedented in the ordinary world. Because these magic horses are themselves (still, at least for the most part) coded, and may be decoded or recoded by someone else (a person who is acting deliberately, directly or indirectly), they are precisely what we would call “the magician’s horse.”

Such constructs as these, common to the code world but without any strong analog to the ordinary world, at least occasionally create a set of objective problems with real consequences and real relationships that ordinary law is systemically unsuited to handle in the code world. It is for this set of cases that there is a need to consider a new sort of law fitting for the new technology; a law for the magician’s horse, reasonably specified to constrain predatory or piratical actors without destroying the power of code for the common good. It is for this reason that I am not only proposing a unified general theory of design to deliberately specify law for the code world, but am actually working out a particular solution to a particular problem that I claim is principled, practical, and predictable. This solution is workable, efficient, and authorized. By testing my general proposal in this manner, I aim to create an actual improvement to a specific law and thereby to validate the general method.

I have much to say about the code world in general and its problems on a large scale. But one has to start somewhere, and I have started with something rather small, and yet highly perplexing to everyone who has tried to grapple with it. My problem for the moment, and for this article, is a coded phenomenon: dynamic focal points in an objective cyberspace, some of which contain trademarks. This problem has bedeviled, confused, and frustrated repeated attempts to deal with it by applying “ordinary principles” of “ordinary trademark law” to the problem. Because the problem is both deceptively common and

35. Easterbrook, supra note 27, at 208.
36. To qualify as analogous or strongly analogous in my usage, the utterance in ordinary space would have to, without more, change the state of an existing thing to some other state. Hence, I do not count such things as legal formulae, robes, or other trappings and shows of conventional semiotics as qualifying. I am looking for “real” magic in terms of objectively operative utterances, repeatable and reproducible on demand in ordinary space to parallel the objective power of code in the code world. I do not find any such thing. But cf., e.g., Jessie Allen, Magical Realism, in LAW AND MAGIC 195 (Christine A. Corcos ed., 2010) (exploring “the American Legal Realists’ critique of law as magic, and its ties to nineteenth century thought” accompanied by words like “legal magic,” “word ritual,” “legal myth” and ritual practice) (footnotes omitted).
actually quite strange, yet one more story might help to shift the reader’s orientation to the fact that this is a coded problem. I turn to Superman for an example, thereby making both the problem of vanity domain names and the outline of my solution to the problem more concrete.

3. Superman Meets Mr. Mxyztplk

The advantage of using vanity domain names to lead consumers to locations in cyberspace is well known. Such domain names feature memorable addresses that act as magnets to draw surfers in otherwise uncharted cyberspace much as a compass might do in ordinary space.

Assume that Martha, unaffiliated with any proprietor of the Superman brand or mark, took a domain name that incorporated the Superman expression. Perhaps her registration of “Superman.com” might afford an opportunity for arbitrage. It might also afford an opportunity for Martha fairly to comment on Bernard Shaw’s *Man and Superman*. It might be an opportunity for her to divert traffic from, hinder or spoil, unfairly to compete, and perhaps to offer goods or services in association with the expression in such a manner as would cause a likelihood of confusion with products offered by the proprietor of the Superman brand (or mark).

Suppose Dank were the proprietor of a trademark related to “Superman” and he were to complain. As I will develop in more detail in the course of this article, it is every bit as easy for Martha to accommodate Dank in this case as in the flowers-that-killed-the-dog example. Imagine Dank were to set up his own website to exploit his own “Superman” brand but without an easily remembered vanity domain name. Let him select “Mr.Mxyztplk.com”—an awful domain name, not easy to guess, pronounce, spell, or to use. At the same time let Martha rewrite her code to alert those visitors to her site that they are just a click away from the “official” Superman site.

Imagine for a moment that such a reasonable technological accommodation were required of Martha by a newly designed law. No user would need to know the backroom technology that engineers the navigation from Martha’s unofficial and unauthorized Superman site to Dank’s official Superman site by the mediation of an unseen Mr. Mxyztplk domain name, but every user would have *ex ante* freedom of choice. No juridical body would need to guess *ex post* whether any appreciable number of reasonable consumers would have been likely to be confused (granting that the offending conduct constituted a “use” actionable under ordinary trademark law). This is because, after a reasonable technological accommodation on Martha’s part, no one could be confused after having been given a fair choice at the point of action. More importantly, no fair-

---

37. Additional information about Superman and Mr. Mxyztplk, including a copy of the comic book art work, a guide to pronunciation and alternate spellings, and other material is in Appendix A, *infra* p. 295.
trading, Superman-dealing Martha would be any more inconvenienced by this accommodation than any nonmurderous, flower-dealing Martha would have been under the previous accommodation. Dank is satisfied at no (or low) cost to Martha. Consumers are satisfied with no significant transaction costs or lost opportunity costs to them; they remain perfectly free to select either Martha or Dank. If Martha really does have any viable and legitimate product to display or some community of interest to serve at her site, some plurality of users will remain to see it. If not, then not. The proof will be in the doing, but each participant will have their own opportunity to fairly navigate in cyberspace.

By removing the unearned and non–value adding opportunity for arbitrage, we have removed the economic incentive to distort cyberspace navigation. By conforming norms to the coded architecture, we have tuned cyberspace to its own specifications. By recognizing a specified focal point offense strictly tied to modest, technologically reasonable coded remedies, we have created the equivalent of a fulcrum and a lever to move the code world. By using the law to construct such a virtual fulcrum, it becomes possible for a virtual lever of now-congruent norms, prices, and architecture to work in support of the deliberate design of a cyberspace characterized by [1] open access, [2] free navigation, [3] reliable information-activity, and [4] a degree of trust necessary to protect otherwise vulnerable [5] augmented presences. All of this can occur at negligible or no marginal cost to any legitimate user.

4. Invisible and Attenuated Uses of Focal Points Some of Which Contain Trademarks

What is happening in the Superman/Mxyzptlk example is new compared to ordinary space. I use that example concretely to identify what is happening more generally with expressions in cyberspace that may contain “invisible” or “attenuated” trademarks, and I will provisionally identify at this point some terms that I will discuss in more detail later in this article. In cyberspace proper, “focal points” are dynamic. They permit navigation, because they may act as navigational markers, like magnets drawing a navigational compass to headings on a map. But dynamic focal points in cyberspace may also be abused or spoiled by offenses that alter the virtual map of cyberspace, plant deceptive markers, ambush a user, or expropriate a focal point otherwise available. These focal point offenses intersect with trademark law. When the offending actor’s marker or spoiler also incorporates a trademark of another person, the 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

---

38. These five characteristics are designed specifications, not accidental attributes, of cyberspace. See generally Folsom, Defining Cyberspace, supra note 8 (deriving a definition from functionally designed specifications).
the essential harm. Fraud 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. This article is about “marker” and “spoiler” offenses against “focal points” in an objective cyberspace. Each of these terms is already within the experience of almost everyone who will be reading this article, but I explicitly name them for ease of reference.

a. Markers and Spoilers.

A “marker” is an expression used as an address or magnet to draw traffic in space. Addresses are well known. Vanity phone numbers (for example, “1-800-callme”) and vanity domain names (for example, “www.this_is_me.com”) are common examples of addresses. Magnets are as familiar. Anything that attracts a human user or a search engine towards a desired location by keyword or other association (“me” as a search term entered into a search engine, returning a list of possible destinations including “this_is_me.com”) can function as a magnet. These all constitute markers because all tend to aid navigation by marking a location itself, or else by pointing toward a desired location.

A “spoiler” is an expression that functions as a roadblock or detour in cyberspace. Roadblocks tend to prevent, and detours tend to divert navigation. These spoilers all oppose navigation because they obscure or hide locations, signs, pointers, or paths towards desired locations in cyberspace.

39. Though perhaps finally going out of style, it has been asserted that actors in cyberspace who use trademarked expressions of another 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 notes 128–148 and accompanying text (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 more fundamental 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.

40. An objective cyberspace is an embodied, coded, and switched network for moving information traffic further characterized by varying degrees of access, navigation, information-activity, and trust among vulnerable augmented presences. It includes the phone system and the Internet, among other things. See infra Part II.B.2. (discussing cyberspace). This article eventually defines the more significant terms in the course of discussing them, but to survey the development of the concepts, one may refer to the prior articles, supra notes 8–11, and a reader who simply wants to make use of the supporting glossaries and summaries may refer to the Appendices of those articles, should see infra Parts III.A–C.

41. 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, for example, “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.

42. 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.
b. Focal Points

“Focal points” are not limited to cyberspace, nor have I coined the term. 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. Here is a common focal point illustration:

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.

It is a short leap from understanding the general power of a focal point in ordinary space to understanding the particular power of dynamic focal points in cyberspace as an aid to, or potential hindrance of navigation. Focal points function as particularly potent markers and as spoilers because of their ability to help or to hinder navigation in space.

The particular power of focal points in cyberspace derives from the fact that 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. Focal points in cyberspace can 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.

Someone wanting to call Holiday Inns to find a Holiday Inn-branded hotel, but not knowing the phone number, might guess a focal point and dial.

---

44. Id. at 47. The game assumes incomplete knowledge, and even though it is 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.
45. Compare THE WIZARD OF OZ, supra note 32 (where Dorothy repeats, “there’s no place like home, there’s no place like home,” while clicking a pair of ruby, or silver, 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 portrayed in a motion picture, as derived from a storybook, and as an imagination or as a shared imagination), while the other actually works in an objective place. The objective cyberspace is real. It is not an imaginary domain, much less a consensual hallucination.
46. The phone system is, after all, an embodied, switched network for moving information traffic, possessed of the other characteristics of an objective cyberspace (access, navigation, information-activity, augmented presences, and trust). See infra Part II.B.2 (defining cyberspace in these terms, and including the telephone system within it); accord Folsom, Defining Cyberspace supra note 8, id. at n.20 (quoting William Gibson, the man who coined the term “cyberspace”: cyberspace includes “the place where a long distance telephone call takes place”).
47. Of course, almost nobody “dials” any more. My nature and place of use analysis is not limited to any specific technology. We don’t need special laws, statutes, or administrative rules of rotary dialed telephones on
“1-800-HOLIDAY,” especially if there has been a promotional campaign making the focal point association. 48 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) might enter the expression “movie buff” or “moviebuff” into a search engine’s search window. Such a person 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. 49 These are uses of focal points as markers in cyberspace because they draw an augmented presence to a location. They act as addresses or magnets.

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 reselling 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. 50 The same sort of targeting might be “noncommercial” but still triggered by focal points and still characterized as an invasive intercept followed by invitation. These are uses of focal points as spoilers in cyberspace because they prevent or

48. See Holiday Inns, Inc. v. 800 Reservation, Inc., 86 F.3d 619, 620 (6th Cir. 1996) (evidencing such conduct on the part of persons seeking to find Holiday Inns, trapped by a deceptively similar mnemonic phone number).

49. See Brookfield Commc’ns, Inc. v. W. Coast Entm’t Corp., 174 F.3d 1036, 1043–44 (9th Cir. 1999) (evidencing two legitimate users of the expression). One party used the expression “movie buff” as part of a composite slogan with a space between the words and subsequently registered a domain name, “moviebuff.com,” without a space between words; the other party thereafter obtained a federal trademark registration for the expression “moviebuff” and then complained about the existing domain name. 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, and ordered the assignment of the domain name from the domain name registrant to the later trademark registrant. Id. at 1049. This particular domain name has apparently fallen into the open market: it is currently offered for sale at a quoted price of $30,000. Contract Form, DOMAINEMARKET.COM, https://www.domainguard.com/cart/contact-information.php?id=moviebuff.com (last visited Mar. 1, 2012) (on file with the McGeorge Law Review).

50. See 1-800 Contacts, Inc. v. WhenU.Com, Inc., 414 F.3d 400, 402–04 (2d Cir. 2005) (evidencing such conduct on the part of persons providing targeted advertising, triggered by typing a trademarked expression of another).
2012 / Poisoned Flowers, Part 1

delay navigation, or provide uninvited information. They act as roadblocks or detours.

Not subject to the same constraints against warehousing or expropriating expressions intended for use as trademarks in ordinary space, focal points can be warehoused, and hence spoiled in cyberspace. Focal points can be spoiled in a special way because, unlike in ordinary space, if a focal point contains a trademarked expression of another, the trademark owner’s goodwill value can be expropriated from its primary user. This is not just a matter of legal reality common to both ordinary space and to cyberspace but of a coded reality specific to cyberspace. In the architecture of cyberspace, if there is only one optimal vanity phone number or vanity domain name, there is no room for anyone else, including a mark proprietor, to use it. If someone takes my trademark in ordinary space and posts it on a billboard, in addition to invoking legal remedies I can still post my mark on my own billboard because ordinary space has an architecture of multiple billboards. But if, as may be the case in cyberspace, there were only one billboard (only one optimal phone number, only one optimal domain name), the offending user poses a double threat: he or she might be infringing my mark, but in addition, he or she has expropriated and prevented my own use of my own mark in that medium. Moreover, unlike simple comparative advertising in ordinary space, focal points can deliver invasive and uninvited invitations from others to a user in cyberspace. Rather than merely thinking my own thoughts about a product category, as might be the case in ordinary space, someone else is capable of invading my thoughts and interjecting their own in cyberspace by coded triggers when my thoughts are embodied within or predictable based upon my actions in a coded world.

Although the presence of a trademark is not essential to the underlying focal point offense, it would seem 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. 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, 51, 52, 53.

51. The United States generally makes federal registration contingent upon use, thereby not allowing any domestic claimant to warehouse unused expressions. See RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 18 (1995) (providing, except for “intent to use” applications under federal law, that trademark rights are acquired only when actually used); Lanham Act, 15 U.S.C. § 1051(a) (2006) (registering marks based on use); id. § 1051(b) & (d) (registering marks based on a bona fide intent to use, contingent upon actual use after a notice of allowance).

52. As to the unnatural attempt to register, and hence to “expropriate” another user’s mark see id. 15 U.S.C. § 1052(d) (providing grounds for refusal to register expressions resembling the mark of another); Paris Convention, 6bis (providing grounds for cancelation of registration of marks that are “well known” marks of another person).

53. But cf. 1-800 Contacts, Inc., 414 F.3d at 402-04 (manifesting an understanding of such things as comparative advertising, nominative or fair use as privileged conduct in ordinary space, but not remarking upon the invasive nature of the intervention in cyberspace).
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\textsuperscript{54} reading of copyrights and “copies.”\textsuperscript{55} Not only has trademark law not yet given up its similar bias, it is currently ill-equipped to do so. My new approach to focal point offenses in cyberspace can reverse the bias and help prevent it from creeping any further into the analysis of trademark-related focal point disputes in cyberspace than it already has.

Trademark’s current difficulty with new technology in cyberspace is not hard to understand. It is a direct consequence of dynamic focal points existing in cyberspace, which are without any strongly analogous reality or corresponding 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 harm when abused.

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 a coded world.\textsuperscript{56} What had previously only 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, and information-activity for those who use cyberspace, including the hitchhiker, surfer, and ordinary folk, and directed towards a common good suitable for public-policy support. The

\textsuperscript{54} White-Smith Music Pub. 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”).

\textsuperscript{55} 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. See id. 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 “although 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 ET AL., COPYRIGHT LAW 67 (8th ed. 2010). See Folsom, Space Pirates, supra note 10, at n.215 (developing this point and crediting Professor Landau for a parallel independent idea, and Professor Heymann for pressing me on the problem).

\textsuperscript{56} Cf. 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.”).
developing laws of any polity containing citizens who are hitchhikers in cyberspace might want to more explicitly consider the benefit to the common good provided by the hitchhiker’s guide before over-regulating coded space.

We can define predatory and piratical conduct in cyberspace, and can distinguish pirates from guides. The distinction turns at least in part on whether they hinder or help navigation by a virtual map. The notion that anyone can blithely alter, destroy, tamper, spoof, block, waste, or ruin navigational beacons to a virtual map in cyberspace any more than “actual” navigational markers and direction signs in ordinary space is odd. Equally odd is the notion that anyone could somehow transform malicious mischief into protected speech or expression because it happens to be instantiated through the operative language of constructed code. To mis-adjudicate either of these in cyberspace would seem as alien and perverse to any rationally designed law for the code world as it would be in any ordinary space in which the same sort of thing could happen.

By way of example, an actor could not alter a “slow down, bridge out” sign and replace it with a “speed up” sign in ordinary space without incurring legal liability. Imagine that a person could simply speak “poison” in ordinary space and then serenely watch all the neighboring dogs die, or could simply speak “friend” and thereby open an impassable barrier and enter. In ordinary space, shouting “fire” in a crowded theater does not itself create any fire. If it did, it would constitute what we would describe as a form of magic or other supernatural 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?

57. See generally Folsom, Space Pirates, supra note 3 (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).

58. For speaking “poison” and thereby making a flower poisonous (or speaking otherwise and thereby making it conditionally nonpoisonous), consider the hypothetical of the poisoned flower in cyberspace in the Preface to this article. See supra pp. 1–3. For speaking a password and then entering, compare not only Ali Baba and the Forty Thieves, supra note 30, but also the journey of the Fellowship of the Ring, TOLKEIN, supra note 31 (opening a door under the inscription “Speak friend and enter” by speaking the word “friend” and then entering).

59. See Richard Ramsey, Perspectives, Mainly Scottish, on Evidence and Procedure in Witchcraft Trials, in LAW AND MAGIC, supra note 36, at 366–67 (noting the repeal in England and Scotland of the statutory offense of witchcraft in 1736, and noting David Hume’s condemnation of the offense as being based upon a delusion; and with the law treading upon a “foul and treacherous” bottom); C.S. LEWIS, MERE CHRISTIANITY, 26 (Macmillan 1960) (1945) (Observing about such speech in ordinary space: “surely the reason we do not execute witches is that we do not believe there are such things” and continuing “if we really thought that there were people going about . . . who were using [supernatural] powers to kill their neighbors or drive them mad . . . surely we would all agree that if anyone deserved the death penalty, then these [traitors] did”). Of course, because those conditions of operative speech 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
Such operative power language is routine in the code world. We can construct poisoned flowers (and we may un-poison them), we may create passwords and can use them to open virtual doors, and we can burn or destroy data by uttering the functional equivalent of “fire” (“delete” would do the trick). From a realistic cyberspace perspective, the problem is easy to identify. There are occasions when coded language produces operative, objective results in a code world. Such language moves or alters information, it changes the state of a machine or of other code, and it delivers an augmented presence from one coded place to another. In such cases, a law for the code world, different from the law for ordinary space, may be the right solution. Dynamic focal points are a prime example. The obvious solution to a focal point offense, once we simply recognize and name the offense, is to encode a reasonable technological accommodation, at least upon request. However, from a traditional trademark perspective, the problem is much more difficult to recognize and the solution much more elusive.

B. The Place of Use

1. The Code World and its Places

It is useful to refer to the coded domain, and to various places within it, as the “code world.” By the code world I signify: an (1) embodied (2) switched (or coded) (3) network (4) for moving information traffic or for changing the state of a machine, a living body, or another coded construct.

---


61. An example of this sort of technological accommodation is the one reached between Martha and Dank which made the poisonous flowers lose their poison when they left 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 supra notes 23–26 and accompanying text.

62. 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.
2012 / Poisoned Flowers, Part 1

Each of the definitional elements is distinctive. The code world is embodied, which is to say objective. It is not a hallucination at all, much less a consensual one. It is “networked” and “switched” to indicate that it is both computational and connected. It is because of the networked and computational connections that code may be propagated from one machine or organism to another, affecting more than a single isolated user. It characteristically is capable of performing at least two functions that make it useful, and also subject to characteristic abuses: it moves information traffic, or it changes the state of another machine or of another coded construct or living body. These same two design features simultaneously create vulnerabilities and the opportunity for offensive, invasive, and uninvited interventions by other actors.

It is a commonplace that there is more than one place within the code world.\(^{63}\) For the purposes of this article, I could have stopped at “cyberspace” as one distinct place within the code world, because it is the only one with which I need to deal at the moment. But the failure to go beyond cyberspace would leave part of the argument unarticulated, creating needless trouble in the related spaces within the broader code world when it comes time to address them.\(^{64}\) I propose distinguishing various places in the code world according to their function, that is, according to the nature of use that answers to the designed specifications that characterize each place. Each is within the larger code world (an embodied, switched network for moving information traffic or changing the state of a machine, a living body, or another coded construct) and each is further characterized by its own designed function within it. These other places, some of which overlap, include at least:\(^{65}\):

1. the *metaverse* as that place within the code world further characterized by the consensual association of like-minded persons (communities of interest);

---

\(^{63}\) Lessig, supra note 1 at 83–85.

\(^{64}\) My approach to problems in the code world is unified and comprehensive. It is also flexible. The reader will notice that my approach to invisible and attenuated trademarks in cyberspace (and my approach to focal points) has a wide scope of “intake” but a very modest and limited remedy in the form of a reasonable technological accommodation. But when it comes time to resolve the different sort of distinctive problems that arise in psiberspace (and the biosphere), for example, the reader will appreciate that the “nature and place of use” will resolve into a different specified rule. In particular, the remedy in psiberspace might be much more “draconian”—the harm in psiberspace may be life-threatening, hence the reasonable notion of permitting robust access and navigation (in cyberspace proper) would yield to the necessity of stopping coded speech that causes death or suffering (in psiberspace). The six places within the code world that I distinguish may indeed overlap, but the key to resolving the characteristic problems of each is to understand the particular functional characteristics at the core of each and to design law according to the differentia. For the particular purposes of this article, five of the six places may be considered to be “orphans” but they reveal something important about the code world and about cyberspace proper. I claim, moreover, that the importance of the other five categories will become more apparent later. See infra text accompanying notes 90–95 (providing examples in the other five domains of the code world, outside the scope of this article, that my general approach will help to resolve).

\(^{65}\) See infra text accompanying notes 90–98 for examples of these places.
McGeorge Law Review / Vol. 43

(2) virtual worlds as those places within the metaverse’s communities of interest, 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) cipherspace as that place within the code world further characterized by a need for trusted, secure, and strong encryption, signature authentication, and verified message content for funds transfer, private, secure, or secret communications and like activities;

(4) psiberspace as the place within the code world further characterized by a human/machine frontier and interaction (and the “biosphere” for coded living matter);

(5) the newspace (or blogosphere) as that place within the code world 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) or where people might arrange to meet or organize to petition their government for the redress of grievances; and

(6) cyberspace (or cyberspace proper) as that place within the code world further characterized by access, navigation, information-activity, augmented presences and trust. 66

I propose the code world as the genus. The other six places are among the sometimes-overlapping species within it. The code world also implicates, and includes, but only in a certain sense (to be explained shortly):

(A) the “new machines,” including virtual machines, code, gateways, portals, pathways, pipelines, biological carriers, bioengineered materials, vectors, hosts, substrates, or other entities that enable the code world;

(B) a range of code world activities from “low” (shallow) to “high” (deep) as well as a bordering range of “peripheral” spaces as a way of characterizing the degree of coded exceptionalism (first-, second-, and third-order problems). Uses in the code world may be considered “low” to the extent they merely mimic or transpose customary transactions from ordinary space to a coded world. These “first-order” problems would seem to be those most nearly solved by ordinary principles of ordinary law and yet are important enough to

66. See Folsom, Defining Cyberspace, supra note 8, at 84–85 (detailing the definition of what I here refer to as “cyberspace proper”).
2012 / Poisoned Flowers, Part 1

have their own name because of some of the odd results that have sometimes confused these first-order cases. A transaction in cyberspace that is unique compared to ordinary space because of the power of code may be said to be in “high” or “deep” cyberspace. A transaction in deep cyberspace may present a second-order problem because of its exceptionalism. This, in turn, may require adjustments of peripheral law, such as remedies or secondary liability, and so may also present a third-order problem;

(C) “transpositional spaces” (or “retrading spaces”) as a set of spaces in the code world characterized either as having, or appearing to have, a low degree of coded uniqueness. These present, or appear to present, a first-order problem by having such a superficial similarity to transactions in ordinary space as to suggest that disputes occurring in space can and should be handled by mere transposition of “ordinary principles” of “ordinary law” to the new technological use. But here it is important to guard against (or at least to be aware of) a tendency to reopen perennial arguments concerning the nature of the “ordinary law” and to “retrade” the outcome, but under disguise or through a failure to appreciate the differences that sometimes creep into the law as if by accident.

The utility of these last three expressions lies in their ability to distinguish a number of confounding variables that are common to all six of the other “places” (the metaverse, virtual worlds, cipherspace, psiberspace, newsspace, and cyberspace proper) within the code world. The category of “new machines” is an explicit reminder that in fact there is almost certainly no need, at least not in the sense I am proposing, for much in the way of a “law of the computer,” “a law of the internet,” or a “law of the biological probe.” These are simply new machines. They are tools to get to the code world. What is of concern is the code world itself, the place in which these tools can and do modify other tools or other code, for good or for ill.

Hence, the “A” category is an aid to resist the tendency to think that there is any inherent or necessary requirement that there be a law of some particular “thing” or system, or momentary technology, rather than a law for the code world itself. If a computer were not networked to other computers, if something propagated on one computer had no effect on any other and could not transmit either active information or state-changing code, then the “law of the computer” would be as sterile as the “law of a horse.” Such a study may provide a legitimate and interesting survey or summary of current law in a topical context, but it is not generative of anything distinctly novel. It is because of the computer’s intimate involvement with a coded world that we care about the possibility of new legal relations affecting them. We often mistake, however, the tool (the computer) accidentally associated with the code world for the code world itself. The law’s
concern ought not to be about the momentary, passing technological means (telephones, computers, tablet devices, or whatever), but about the massively looming phenomena, unprecedented in the collective experience of humankind: the code world itself. The new machines are fascinating, of great interest to the curious, the hobbyist, the engineer, and entrepreneur, but no judge anywhere ought to suppose a mastery of electrical engineering, recombinant DNA, or network topology is the key to resolving the problems of the code world. What is needed, and what I am proposing, is a technologically sensitive approach that is not bound by law to any one technology. I claim my proposal will still be relevant, useful, and productive for generating solutions to problems in the code world even after all current technologies for accessing the code world are obsolete. I claim my proposal will continue to work for as-yet unanticipated technologies within the code world.

The B category, low-to-high and peripheral effects, encourages thinking about degrees of cyberspace or of anywhere else in the code world. It complements the foregoing presumption that there is not necessarily any need for new laws for new machines, but rather a new law for the code world in some cases. The B category is an aid to resist any tendency towards an automatic response once we get to the code world. A first-order problem in low cyberspace might very well be handled by ordinary principles of law already developed over years (or centuries) of experience in ordinary space, but second-order problems not so much. It is just as wrong to treat a second-order problem as if it were a first order as it would be to overreact to a first-order problem. The category of third-order, or peripheral, concerns, is explicitly meant to force an answer to questions and objections that could derail a poisoned flowers solution. Someone might object, for example: “you’ve just expanded the zone of substantive liability to those who grow flowers, do you mean to put flower growers out of business by imposing upon them crippling remedies borrowed from the law of nuisance?” Or again, it might be objected: “you’ve just expanded the zone of direct or primary liability related to flowers, do you mean to put the plant supply, fertilizer, delivery, and payment system businesses under crushing secondary liability rules?” The answer to both questions is “no.” The answer is “no” because the coded remedies are logically and inherently limited to reasonable technological accommodations, and secondary liability is likewise limited. These are not fanciful objections. They deserve an answer, and the distinction among first-, second-, and third-order problems will provide appropriate answers.

The C category, transpositional or retrading spaces, focuses on the surprising results accompanying first-order problems. It encourages the explicit step of asking whether any particular act in the code world might be nothing more than an ordinary transaction merely transposed to the code world, and yet not stopping there until asking some further questions about “retrading” the same doctrinal deal in the code world that was previously struck in ordinary space. We might purchase a widget over the counter at a store, or with later technology by mail
2012 / Poisoned Flowers, Part I

order accompanied by a personal check through some sort of catalog, then by telephone with the aid of a credit card, or later through an on-line store by way of a click-through and an associated payment system. It certainly seems there is no need for a new law of contract for each new technology. All these do is enable each of the successive transactions, each transposition being essentially like the others before it. The telephonic and on-line permutations would each seem to be merely “transposed” transactions in a transpositional space within the code world.

Yet it is also important to keep in mind the countervailing category of “retrading places,” if only to double check against hidden or disguised variations of established law, “retraded” in the code world while the claim is made that this still constitutes “ordinary principles” of “ordinary law.” It is surprising how many folk seem to think that there ought not to be legally enforceable disclaimers or limitations of warranties printed on the back of hat claim checks, parking lot stubs, or airline or passenger-ship tickets. It may be that they press their nonacquiescence in ordinary space into cyberspace. It sometimes seems that this appeal to “ordinary principles” proceeds as if the existing doctrines concerning, for example, allegedly “newly proposed terms” that are often not “new” at all, but terms well understood and customarily included (and that could be declined more or less readily) had not been worked out in ordinary space. And the argument proceeds as if doctrines relating to contracts of “adhesion” that contain terms economically reasonable and useful had not already been worked out as well. By this form of argument, any number of standard doctrines and their standard exceptions suddenly seem to disappear in cyberspace. It is as if the “shrink wrap” or “click through” in cyberspace were something outrageous, despite routine examples of enforcing analogous relationships as a matter of course in ordinary space.

In fact, it is hard to avoid the impression that there are some law reformers trying to retrade in cyberspace the balance already struck in ordinary space. Consider taking a doctrine of “ordinary law,” such as offer and acceptance, forgetting the ordinary exceptions and ordinary reasoning already worked out in ordinary space, and tempting juridical agents simply to apply “ordinary principles” of “ordinary law” to cyberspace while in fact incidentally reversing those principles.\(^67\) Of course, I am not opposed to the dynamic growth of the law, but I am opposed to indirection and failure to clearly identify the arguments and

\(^{67}\) Compare ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1451 (7th Cir. 1996) (Easterbrook, J.) (resisting such temptations and enforcing license terms contained within the package of shrink-wrapped software by analogy to ordinary law: “[t]ransactions in which the exchange of money precedes the communication of detailed terms are common. Consider the purchase of insurance . . . . an airline ticket . . . . a ticket to a concert . . . . a radio set . . . . [s]ugs . . . . [and] the software industry itself.”), and Hill v. Gateway 2000, Inc., 105 F.3d 1147, 1149 (7th Cir. 1997) (Easterbrook, J.). (extending the holding in ProCD from licensed software to purchased hardware: “ProCD is about the law of contract, not the law of software”), with Easterbrook, supra note 27 (no need for any special law of horses, or of software or computers).
trace the consequences in the coded world. The code world does have much to teach, and it could highlight certain existing problems in the law of ordinary space. I claim only that the technique of re trading would be better exercised if it were frankly acknowledged as such.

2. An Objective Cyberspace Within the Code World

The code world is a large domain. I identify it here for the sake of context. Cyberspace is but one place within the code world. Yet that is the place of the narrower subject of this article. It is where the particular problem I am addressing arises. Focal point offenses occur in an objective cyberspace. For rule-specific purposes, an objective cyberspace may be defined as:


Cyberspace includes the Internet, the phone system, probably Wi-Fi, and much of digital radio and television. It is aptly observed that what is commonly called “cyberspace” (by others) is really a number of different places. There are observable and different characteristics in each functionally distinct place. Yet, these different places within the code world, including cyberspace proper, all have one thing in common despite their individual differentia. All of them, together with coded places not yet named or developed, are part of an embodied

68. There are many perspectives from which to consider “cyberspace,” but this perspective is productive for the purpose of finding a public good that 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. See Folsom, Defining Cyberspace, supra note 8, at 85–87.
69. Id. at 87–92.
70. Id. at 84.
71. Id.
72. Id. at 84, n.21.
73. Folsom, Non-Neutral Principles, supra note 11, at 43, n.3.
74. See Lässig, supra note 1, at 82–83 (describing a number of “cyberplaces,” each providing a different experience). In contrast, I have defined cyberspace as one place within the larger code world.
75. See supra text accompanying notes 64–66 (in my usage, these distinct places include at least: the metaverse, virtual reality, cipherspace, psiberspace, and cyberspace proper, as well as newsspace); Folsom, Non-Neutral Principles, supra note 11, at 43, n.3.
76. All of these places are unified by the fact that they are created by code and yet are differentiated by each having their own reasons for being and their own specific sets 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.
2012 / Poisoned Flowers, Part 1

switched and coded network for moving information traffic or changing the state of a coded construct, machine, virtual machine, a living body, or other code (the “code world”). The code world is enabled, accessed, and navigated by way of machines or devices (the “new machines”), and by pathways or pipelines that permit and encourage new technological uses in the code world.

I may summarize the definitions already given as follows, narrowing them to the point of this article and now explaining the significant policy implications. According to my usage, the broadest and most expansive domain is the code world. The code world contains within it at least a half dozen functionally designed places, one of which is “cyberspace” (or “cyberspace proper”), a narrow place within the code world characterized by varying degrees of (1) access, (2) navigation, (3) information-activity, (4) augmentation, and (5) trust.  

These five designed characteristics of cyberspace also constitute a straightforward catalog of reasons why people value the place. Because they admit of degrees, these five characteristics can describe a range of cyberspace, from “low” or “shallow” (implicating the characteristics to only a limited extent) to “high” or “deep” (exhibiting the characteristics to a far greater extent). It is in high cyberspace that the focal point offenses tend to manifest themselves as second-order problems. They provide a rational basis for predicating (positing) a public policy, or common good, in cyberspace.

Laws or policies that promote robust access, reliable navigation, retrievable and active information; protect augmented presences from the special vulnerabilities faced in space; and foster at least the minimal level of trust necessary to the use and enjoyment of space are “good” for cyberspace. The contraries are, other things being equal, “bad.” As a normative and policy matter, the law ought to be designed to promote the common good and to

---

77. The five characteristics may be objectively determined. 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, which 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 8, at 87–91.

78. 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.


80. Id.
discourage what is bad for cyberspace. The notion of “low” to “high” and “peripheral” may be more definitely exemplified for purposes of legal analysis by characterizing particular legal problems in the code world as first-, second-, or third-order problems. I am not here dealing primarily with first-order problems that really are merely transposed from ordinary space and which usually may be resolved by ordinary principles of ordinary law. Such problems are not trivial, but they are not the focus of the paper. Instead, I am concerned about dynamic focal points in cyberspace, some of which contain trademarked expressions, precisely because these raise second- and third-order problems that are as yet not recognized and also threaten catastrophic legal failure in cyberspace unless they are recognized and addressed.

Cyberspace proper is important because it embraces the Internet, the phone system, Wi-Fi, and much of modern digital radio and television. It is not important because of the new machines that enable or access it—cyberspace is not simply “the computer” or “the Internet” or any particular technology—but because of the objectively designed functions, effects, relationships, and applications enabled by the new machines in cyberspace. These are among the most useful, enjoyable, and commercially valuable applications presently manifested within the code world. Moreover, 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 shallow code world and in low cyberspace are merely first-order problems transposed from ordinary space to cyberspace. Just as there may be no need of any special “law of the horse” in ordinary space, so in many cases, there may be no need of any special law of cyberspace. Instead, 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

81. Id. at 908 & n.248. See THOMAS AQUINAS, SUMMA THEOLOGIA, Ia-IIae, Q 90, a 2; Q 94, a 2 (Alfred J. Freddoso trans., 2009) (observing that every [good] law is directed towards the common good, and that “the good” is what “all things desire”).

82. Such first-order problems include the potential creation of a trademark or service mark intended for use in ordinary space by use in cyberspace (with or without sales of any particularly branded product), and the geographical priority attaching to any such designation; or the creation of trademark-protected brands associated with virtual goods or services rendered in virtual worlds. Consider, for example, “Instapundit” as used by Glenn Reynolds for his blog. Reynolds, supra note 23; and the designer labels and architectural works described by Professor Lim. Lim, Virtual World, Virtual Land, but Real Property, supra note 94. Such problems will put pressure on the proscriptions in ordinary space against creation of trademark rights by “mere” advertising, by “mere” pre-announcement of products (including vaporware), or by designations used but not associated with anything that is specifically offered for sale with the designation associated or affixed thereon.

83. Folsom, Defining Cyberspace, supra note 8, at 84 & n.21.

84. See Folsom, Non-Neutral Principles, supra note 11, at 47 n.5 (“I do not claim that there needs to be a law of ‘cyberspace’ (or a law of horses”) Cf. Easterbrook, supra, note 27 (pointing out that the law of contracts, property, or tort might be all that is necessary to understand legal relations in or affecting horses—there is no need for any “law of the horse”—and asserting there is no greater need for any “law of cyberspace”).

229
of the code world can be changed simply by rewriting the code. My approach articulates the difference by distinguishing the times and places in which a newly designed law suitable for cyberspace, or anywhere else in the code world, really is necessary.

3. Advantages of the Place of Use Analysis

The advantage of explicitly recognizing a “place of use” analysis is that it allows us not only to locate the conduct as within the code world, but also to locate it within a particular place having functional, deliberately designed characteristics such as, for the purposes of this article, cyberspace. The analysis I propose permits fact-finding on the basic issue: is the conduct even “in” cyberspace at all? It also recognizes varying degrees of cyberspace. In “low” or “shallow” cyberspace, there may be much less need of a special law for cyberspace. Additional advantages of explicitly defining cyberspace as a potentially significant place are threefold. First, new technological uses (NTUs) in the code world and cyberspace “are something like the law’s canary and might provide an early warning to the existence of problems otherwise latent in the law.” Second, NTUs in the code world and cyberspace “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.” Third, and finally, “NTUs in the

---

85. See also Folsom, Non-Neutral Principles, supra note 11, at 47 n.5: I claim only that there should be a law that is suitable for cyberspace (just as it would be fair to ask whether existing laws are, or are not any good for persons who want to buy, sell, ride, use, own or rent horses, or for those who might be kicked by, bitten by, or need to clean up after them). The difference in emphasis between a law of and a law for cyberspace and the code world might be a small one in the beginning, but it is significant and increasingly so as further implications are drawn from it.

86. A shopper who picks up the phone, calls a catalog vendor at the number indicated in the catalog, and orders a shirt is using the phone and so is in cyberspace. But the transaction is in “low” or “shallow” cyberspace to the extent it looks like an ordinary purchase transaction simply transposed to cyberspace. So a person who browses a web site in cyberspace and sees visual copy that includes a trademark used in space pretty much like any trademark used in any other media is in “low” or “shallow” cyberspace. An explicit consideration of the place of use permits both the opportunity to ask whether there is anything in the particular transaction warranting special treatment by legal rules, and also the opportunity often to answer “no” and occasionally to answer “yes.” The new factor permits the question to be raised and demands that it be answered before taking the next step.

87. Folsom, Non-Neutral Principles, supra note 11, at 47 n.6

88. Id. at 47 & n.7 (explaining how “any changes to the law can be confined to the code world (so as not to create any sort of undesirable [and unanticipated doctrinal creep or] ‘feedback’ loop that might upset settled law in the ordinary world where the costs of compliance might be substantially higher than in the code world”)’). What is needed, in short, is not a hammer, but a lever (and a fulcrum). See infra note 118 and accompanying text (illustrating the failure of current trademark law’s hammer).
code world and cyberspace are important because the possibility of spectacular juridical error is non-trivial and perhaps highly likely.”

C. Designing Law: Combining the Nature of Use and the Place of Use

In any analysis of any nontrivial problem in the code world, one significant advantage of combining an explicit consideration both of what exactly is happening and where exactly it is happening is that the combination leads to a working principle: the “nature and place of use.” I call this a working principle because it is rule generating. It works on the level of general principle (or standard), as a rule of thumb or heuristic, to reorient juridical thinking when confronting the problem of whether, and if so, how exactly to design a law appropriate for a coded world. It works also on the level of rule-specified application. In any given particular context, the general principle may be refined, tuned, focused, and developed into a specified rule appropriate to the context. After a very brief outline of its application to the more general set of problems in the larger code world, I turn to the much more narrow problem of using the nature and place of use to design rules for dynamic focal points in cyberspace.


A reader, especially one with a healthy skepticism toward academic theorizing, might well wonder at the amount of apparatus that has so far been introduced into this article. To the contrary, my claim is that everything advanced thus far is both commonplace and necessary to name in order to make useful distinctions. It is time now simply for some examples that will directly demonstrate the use of the categories I have named. Let me propose some examples of near-magic within the code world, from beginning to end, from alpha to omega:

(α) an actor intercepts signals emanating from a nanotech medical device implanted in another person and inserts code . . . ;

(β) an actor thinks it would be fun or profitable to break the encrypted code of a bank account, the commercial electronic funds transfer system (the

89. Id. at 48 & n.9, citing Folsom, Space Pirates, supra note 4, at 873–76 (“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”).

90. This is a problem in psiberspace.

91. Many examples could be given, but in honor of the provenance of the word, “cyberspace,” see GIBSON, supra note 60.
so-called wire transfer system), or to hack a remotely controlled military weapon or a “smart” automobile . . . ;

(γ) in a time when there are logo-bearing garments, road signs, and commercial signage illuminated by embedded LED-like devices, an actor flips the electronic switches so that the logos, directional and warning signs, and commercial signage display different messages as the actor pleases . . . ;

(δ) in a virtual world, an actor inserts disruptive code that terminates avatars, defaces the aesthetics, loots virtual property, or counterfeits virtual money for use as a medium of exchange in coded space regardless of whether such conduct violates the terms of any end-user license agreements and regardless of whether any other player is in “privity” of contract . . ;

92. These are problems in cipherspace. See U.C.C. § 4A-203(a)(2) (2009) (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, identifying 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 Apr. 9, 2010) (on file with the McGeorge Law Review) (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”]. . . . [T]his development would render any cryptosystem based on these one-way functions insecure and useless.”) (emphasis added)); Siobhan Gorman & Evan Perez, FBI Probes Hack at Citibank, Russian Cyber Gang Suspected of Stealing Tens of Millions; Bank Denies Breach, WALL ST. J., Dec. 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 that allegations of a breach of Citibank’s systems and associated losses are false (emphasis added)); Siobhan Gorman, et al., Insurgents Hack U.S. Drones, WALL ST. J., Dec. 17, 2009, at A1 (describing intercepts of unencrypted code generated by an armed weapon system in flight).

93. These are problems in the metaverse. The examples given here are based on the programmable “loglos” (presumably, logos that glow) envisioned in the metaverse created, so far, only in fiction. See generally NEAL STEPHENSON, SNOW CRASH (1992), and id. at 469–70 (recounting the invention of the term “metaverse” and the pertinence of Apple Computer’s Human Interface Guidelines in constructing it). For an early work on some of the legal issues arising out of geographic information systems, see Harlan J. Onsrud & Robert I. Reis, Law and Information Policy for Spatial Databases: A Research Agenda, 55 JURIMETRICS J. 377 (1995) (pointing to promises of efficiency, dangers of loss of privacy, and the underdeveloped state of the law).

94. These constitute further problems in the metaverse. In fact, the proposed solution to the Martha–Dank poisoned flowers problem with which this article began, 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 not only a particular game suboptimal equilibrium, but 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 would have to replace each sophisticated or “trained” dog with a new dog having certain primitive methods; perhaps 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 A.T. Fairfield, Anti-Social Contracts: The Contractual Governance of Virtual Worlds, 53 MCGILL L.J. 427, 429 (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. 232
(ε) in a coded world, it is possible to read text in a first jurisdiction that was created in a second jurisdiction; the libel law of the 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. . . ;

(ζ) in an effort to produce an index to a library in a coded world, a computerized agent reads, stores, and recalls copyrighted material for future reference, including the contents of an entire book, but the law of copyright prohibits unauthorized reproduction of copyrighted material, thereby discriminating against machine memory (or else putting human memory equally in jeopardy of liability for its retention of an unauthorized copy in the mind/brain); in a coded world, language creates virtual machines, compositions of matter, or “processes” and the law of patents seems to include such things within the category of patentable subject matter . . . ;

(intervening illustrations η–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

737 (2007) (proposing zones of exclusion in virtual worlds, where all advertising would be prohibited); Yee Fen Lim, Differing Conceptions of Trademark Infringement in the Virtual World and the Assumption of Multiple Parallelism, presented at the Intellectual Property Scholars’ Conference (Aug. 7, 2008), abstract available at www.stanford.edu/dept/law/ipsc/pdf/lim-yee-fen-ab.pdf (on file with the McGeorge Law Review) (challenging the assumption that the intellectual property regime as it exists in the real world can be carried over into virtual worlds such as Second Life with only some minor adjustments required); Hannah Yee Fen Lim, Virtual World, Virtual Land but Real Property, SINGAPORE J. LEGAL STUD. 304 (Dec. 2010) (considering the legal concept of land in virtual places such as Second Life, independently of intellectual property law).

95. These are problems in the blogosphere. See, e.g., L. Gordon Crovitz, A Town Called Sue, WALL ST. J., Dec. 21, 2009, at A19 (“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.

96. These are yet further problems in cyberspace, in addition to the trademark-related focal point problems with which I am concerned in this article. If it is supposed that a human reader’s mind or brain does not “reproduce” an unauthorized copy of copyrighted material, it is hard to see how, apart from “retrading” the result, this becomes a prima facie case of copyright infringement when accomplished by a new machine in cyberspace. If patent law’s subject matter includes verbal or coded constructs, it is hard to see a stopping point in ordinary space at which the (patentable) machine or process becomes a virtual machine or technologically enhanced thought-manipulation process and crosses the line into (unpatentable) laws of nature, abstract ideas, or simple building blocks already in the public domain and the exclusive property of no one.
2012 / Poisoned Flowers, Part 1

by the targeted person . . . (not to mention any implications of fourth-generation warfare). 97

And we might also include the corresponding problems of secondary liability throughout the code world. 98

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

2. The Nature and Place of Use: Dynamic Focal Points in Cyberspace

Cyberspace proper is a domain designed for open access, free navigation, and reliable and near-immediate active information, used by vulnerable augmented presences requiring a measure of trust. One problem is that the “place” (cyberspace) contains billions of addressable locations, but it has no physical map. Instead, as if by a hitchhiker’s guide, some measure of navigation is possible by way of a virtual map. I base my focal point claim on the foundational proposition that the map to cyberspace is extraordinarily valuable; it is a necessary condition to the efficient working of cyberspace.

---

97. This includes the public laws, privacy laws, and Fourth Amendment issues identified by Professor Lessig. See Lessig, supra note 1, at 44–46 (reexamining the telephone wiretap cases in the context of cyber searches and underlying principles). Amir Efrati & Siobhan Gorman, Google Mail Hack Is Blamed on China, WALL ST. J., June 2, 2011, at A1 (discussing hacking attacks on Google Gmail accounts, including those of dissident People’s Republic of China nationals, as well as the possibility that the PRC was responsible for the attacks); James T. Areddy, Beijing Fires Back at Google, WALL ST. J., June 21, 2011, at A19 (reporting on China’s denial of any involvement in the attacks against Google). See generally RUSSELL L. WEAVER, FROM GUTENBERG TO THE INTERNET: FREE SPEECH, ADVANCING TECHNOLOGY, AND THE IMPLICATIONS FOR DEMOCRACY (forthcoming 2012) (examining the Internet’s impact in shaping political debate, action, and social change).

98. 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 11, at 97 n.172 (listing some of the adverse effects of such extended secondary liability in the code world).
If there were any public policy, or any common good, to be discovered in cyberspace, I claim that ensuring the basic integrity of the map is such a thing. By considering the nature and place of use of dynamic focal points in an objective cyberspace, it becomes possible to consider not only the good that they produce by mapping the place with markers and addresses as aids to navigation—activities generally to be supported—but the harm they may cause if misused. I am able, that is, to convert a general principle (a standard) into a rule-specific form. I claim I can distinguish pirates, predators, and parasites on the one hand from value-adding resource providers on the other. Incidentally, I can also take into account the needs and desires of ordinary users. Now it becomes possible, in a few words, to state the specific actions that cause problems with focal points in cyberspace. It is precisely because they have no real precedent in ordinary space that it is necessary to have a rubric (the nature and place of use) that will reframe the question, identify the problem, and generate a reasonable resolution.

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 alters a warning sign. For spoofing, imagine a calculated misrepresentation of the identity, location, or nature of a landmark. For ambushing, suppose it is possible for someone to listen in to your cell-phone conversation and then subsequently to start whispering in your ear, to insert invasive 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). For spoiling, think of a medium in which only the first person to register a word, including existing words as well as newly created ones, could effectively use it.

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. The power of code to change the state of the coded construct is an additional reason to focus the discussion on the general nature of the offense by paying attention to what is actually happening in cyberspace.

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 waste or ruin the map. The spoiler might warehouse and so prevent someone else from using otherwise-salient focal points, as a roadblock; or might delay or hinder a user in arriving at an intended destination, as a time-wasting detour. The spoiler can effectively expropriate, spoil, or waste an associative focal point, preventing its effective use by anyone else, and especially including the person who might have created the association. Dynamic focal points can do all these things in cyberspace. Offending users have done all of these things with focal points in cyberspace. The law has been ineffective in responding.

The focal point analysis I am proposing recognizes that 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 Technique: Designing Rules for Magic Horses

The technique of using the “nature and place of use” to design legal rules in the code world is neither difficult nor esoteric. First, ask whether the conduct is in the code world at all, and if so, where exactly: does the conduct merely involve a new machine in a transaction simply transposed from ordinary space (a “first-order” application), or does the conduct present a uniquely coded problem in deep space manifesting a “nature and place of use” that is characteristic of the code world and unprecedented in the ordinary world (a “second-order” problem)? Second, ask about ordinary law. It is helpful to examine the most nearly applicable legal rules developed in ordinary space to see whether they could apply either directly or by some careful adjustment, or whether they exhibit a systemic failure to handle the recurring problems arising out of the new nature and place of use in the code world. Third, if the conditions are right, the “nature and place of use” analysis may be invoked again, this time to determine a specified rule to resolve the problem in light of both the second-order problem presented and also any peripheral (“third-order”) considerations. Before finishing any second- and third-order adjustments, and at the periphery, the legal remedy

103. This is simply to restate the dynamic power of code in a coded world.
104. These are commonplace occurrences, within the experience of almost everyone reading this article. See generally Folsom, Missing the Mark, supra note 9 passim (recounting examples from adjudicated cases).
105. Id.
McGeorge Law Review / Vol. 43

should be tailored, proportionate, and limited to reasonable technological accommodations; and any potential secondary liability implications must be likewise limited. Among the third-order issues to be considered are relations with other, cognate legal regimes that might incidentally affect the subject matter of the new technological use.

I claim that, where possible, we should deliberately design legal rules for new technological uses to coincide with the other factors (norms, markets, and architecture) that influence conduct. 106 Given the ability purposely to choose our design in the case of the focal point offenses I propose in this article, I claim that we should design all of these factors cooperatively to support the foundational values 107 of cyberspace under a specified and unified theory. Once that happens, and as we develop a law deliberately designed for cyberspace, 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. 108

I am concerned about the case in which Martha, or any other originator of poisoned flowers (or any other offensive coded construct), might say to the friend of the dead dog or of the Superman brand (or of any other thing impacted by offensive code) something to this effect: “No. You cannot make me. I will not recode nor will I do anything else to help you.” 109 I am equally concerned with the case in which Dank, or any other opportunistic plaintiff in Dank’s position,

106. See LESSIG, supra note 1, at 85–99 (positing these influencers of conduct).

107. These “values” are precisely the ones I have already mentioned briefly in this article—access, navigation, information-activity, and trust sufficient to enable augmented presences to roam about (or surf) cyberspace. See supra notes 8–16 and accompanying text. I have also discussed them at length elsewhere. See Thomas C. Folsom, Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality), 9 TUL. J. TECH. & INTELL. PROP. 75 (2007). It is because of having first specified the function of cyberspace that it becomes possible to speak intelligibly of good or bad, legitimate or illegitimate users of cyberspace, all relative to the designed specification. I claim no monopoly on the specification, but merely claim there is one and that I have proposed an explicit and reasonable definition suitable for legal work. Let anyone else propose their own, but let us require as a condition to designing intelligible legal solutions in cyberspace that there at least be some specified definition of the thing we are trying to design.

108. 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 Martha had simply recoded her offending flowers in cyberspace.

109. See supra note 25 and accompanying text. 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 would not need many laws. The problem for law resides in precisely the set of cases in which someone in Martha’s position refuses to remedy the harm. Because the 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.
might demand too much (more than needed to resolve the problem) thereby threatening to cripple the code world. Norms having failed to influence the desired response from the offending party (or the opportunistic victim)\footnote{Cf., e.g., Graeme B. Dinwoodie, Private Ordering and the Creation of International Copyright Norms: The Role of Public Structuring, 160 J. INST. & THEORETICAL ECON. 161 (2004) (discussing norms generated by Internet service providers and by digital rights management systems); Jacqueline D. Lipton, Bad Faith in Cyberspace: Grounding Domain Name Theory in Trademark, Property and Restitution, HARV. J.L. & TECH. (2010) (discussing norms generated by the concept of bad faith); Dotan Oliar & Christopher Jon Sprigman, There’s No Free Laugh (Anymore): The Emergence of Intellectual Property Norms and the Transformation of Stand-Up Comedy, 94 VA. L. REV. 1787 (2008) (discussing norms generated by the community of comedians). Of course, if humankind were composed of (good) angels who therefore invariably followed normative virtues then, as the argument goes, we would not need many laws at all. See THE FEDERALIST No. 51, at 163 (James Madison) (Encyclopedia Britannica ed., 1952) (“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 “sic utere tuo ut alienam non laedes” principle (so that Martha might “so use her own” coded flowers “as not to disturb” Dank’s coded dog by killing it, especially when Martha may do so at essentially no cost).} this response from Martha or Dank would throw the offended party back upon “ordinary” law for recourse.\footnote{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 application of old doctrines where they manifestly do not 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.} Yet there might not be any obvious or easy recourse under ordinary pre-existing law. Instead of ignoring the problem or haphazardly stretching or distorting ordinary law to accommodate the unusual, extraordinary characteristics of the code world, I claim that a purposefully transformed law for the code world can provide a surprisingly easy rule of thumb that 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 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 to start actually choosing solutions and resolving the characteristic problems of cyberspace. What, indeed, will we do with poisonous flowers\footnote{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. See, 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 BEAULDELAIRE, LES FLEURS DU MAL (Richard Howard trans., David R. Godine ed., 1982) (1857) (pointing by metaphor to dangerous flowers whose consequences linger and cannot easily be coded or wished away); Lu Ting-yi, Dir., Propaganda Dep’t of Cent. Comm. of Chinese Communist Party, Let Flowers of Many Kinds Blossom (May 26, 1956) (often attributed to Mao Tse-tung and rendered as “let a thousand flowers bloom”) (on file with the McGeorge Law} and other coded constructs 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?” On the other hand, what if Dank were to convince some judge or other juridical agent to impose a needlessly high tariff on code itself, to the disadvantage of everyone who depends upon the success of the code world? The poisonous flower in cyberspace is no metaphor at all, but real.\(^\text{113}\) It is real code that constitutes the properties, functions, and methods of the coded flower (and any number of other coded constructs), and such code really can be changed to affect the objectively observable nature, characteristics, and qualities of the resulting flower.

The poisoned flower hypothetical is an example, not of some figure of speech applicable to cyberspace, but of the different reality of words uttered in the code world and cyberspace, compared to words in “ordinary” space. Coded constructs are objectively real in the code world. This changes things. This is no longer an ordinary flower (or a horse), and this is no longer a question of whether there should be a law of the flower (or a law of the horse), \textit{simpliciter}. In the code world, there are at least some cases in which the horse is not only a horse of a different color, but a horse of a fundamentally different nature. For at least some code-world-exceptional consequences of coded constructs, we need a deliberately designed and transformed law.

This article is part of a larger project to specify and design contemporary legal solutions based on a common morality for a global and technological age.\(^\text{114}\) This article concerns the tech side of the project, and so it will share some of the features of the coded world it describes.\(^\text{115}\) It is a coded world, after all, that the law is seeking to regulate. In “holding the mirror up” to this coded “nature” it is

\(^\text{113}\). 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.


\(^\text{115}\). This article is built in a step-wise modular fashion; moreover, it tends 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 have 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, \textit{OH! PASCAL!} xiii (2d ed. 1992). I hope to produce “a presentation that’s detailed enough for [experts], yet lucid, readable, and enjoyable enough for [interested nonexperts] to read . . .” \textit{Id.} at xv. As the good professor declares, “if YouCanReadThis then begin.” \textit{Id.} at xxi.

This article also includes a number of “Easter eggs”: “hidden messages, in-jokes, or features” embedded in the media—some in the footnotes and some in the main text. \textit{See Easter Eggs (media), WIKIPEDIA (last visited Feb. 2, 2012), http://en.wikipedia.org/wiki/Easter_egg_(media) (on file with the McGeorge Law Review) (defining the term and giving some well-known examples). See supra note 5 (alerting the reader to some of the Easter eggs in this article).
2012 / Poisoned Flowers, Part 1

well to remember two apparently contradictory tendencies. First, any mirror image is reversed and so is similar to, yet different from, the original image. Second, real things in the code world sometimes work pretty much like the way things work in the ordinary world, but sometimes they work in ways that are distinct and make a difference. Where things are very nearly the same, nothing much needs to change; there is no need for a law particular to the coded horse when it behaves rather like an ordinary horse. But when objective relationships are fundamentally different in the code world, then it is time to respond in a more suitable way, by a transformed law purposely designed to be more fitting to the good or ill that a coded horse might realize or wreak.

D. When Trademark Fails

If existing trademark law could resolve the problem of dynamic focal points in cyberspace, some of which contain trademarks, there would be no need to propose either a new focal point offense or a revised trademark law to accommodate the problem of likelihood of confusion caused by invisible and attenuated uses. But current trademark law does not resolve the problem, nor can it. I have written more than one prior article to make that point, so I might take it as an established starting place for this article. 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 (a “trademark” way of describing focal point offenses) in an objective cyberspace.

I present here a condensed version of the statement of my position (additional comments are elsewhere in the body of this article). I maintain, first, that no one has explicitly addressed the problem of dynamic focal points at all. I maintain, next, that traditional trademark law faces three obstacles in respect of new technological uses in cyberspace. The first is the threshold “initial interest” obstacle, which results in overprotection of many marks in space by wrongly elevating “initial interest” from a common fact to a nearly dispositive inference

116. Compare William Shakespeare, Hamlet act 3, sc. 2 (noting that 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, in The Annotated Alice: Alice’s Adventures in Wonderland & Through the Looking-Glass 129, 144 (Martin Gardner ed., 2000) (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 1 Corinthians 13:12 (warning that ordinary space itself is not entirely clear, “[f]or now we see through a glass [a mirror], darkly”). See generally 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).

117. See Folsom, supra notes 8–10 (referencing my trademark-related articles). All of these are available on the Social Science Research Network (SSRN) at http://ssrn.com/author=519369. The reader who wants to see a detailed analysis of specific cases may refer to those articles, especially Missing the Mark, supra note 9. This current article stands on its own, but is not entirely complete without some reference to the others.
of liability. The second is the threshold “no-use” obstacle, which results in under-protection of many marks in space by wrongly seizing upon the absence of conventional “use” (and dismissing the claim altogether). The third obstacle constitutes the very real problem of making some rational assessment of “likelihood of confusion” in the context of an invisible or attenuated new technological use of an expression that contains a trademark, once it is determined that neither all nor none of the offending conduct can be determined at the threshold by either the initial interest approach or by the no-use approach.

Traditional trademark law provides a toolbox that contains only a hammer when the target might not be a nail. 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 expressions purposely constructed in a coded world to draw or block traffic, notwithstanding the 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, complementary, 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? Moreover, even if an invisible or attenuated use could do so, how would anyone know how to recognize it according to any useful legal test? What follows in the next parts of this article is a compressed version of some arguments I have made elsewhere, together with some new elaboration.

1. Failed Gatekeeping Rules

Overprotection and “initial interest.” It is not at all surprising that one line of trademark cases responded to these riddles by embracing one incorrect extreme.

118. 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: A RECONNAISSANCE 15 (1969) (“I suppose it is tempting, if the only tool you have is a hammer, to treat everything as if it were a nail.”); PETE SEEGER & LEE HAYES, IF I HAD A HAMMER (THE HAMMER SONG) (TRO-Ludlow Music, Inc. 1949) (“If I had a hammer I’d hammer in the morning, [and] I’d hammer in the evening all over this land . . . Well, I’ve got a hammer . . . it’s the hammer of justice . . . ”). One would hope the “hammer of justice” might hit some “nail” calculated to mend some specified instance of injustice 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.

119. I use two expressions almost interchangeably, but based on the perspective. From the perspective of cyberspace, the activity involves dynamic focal points that are markers or spoilers used as addresses, magnets, 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.
2012 / Poisoned Flowers, Part 1

This first line of cases over-protects trademarks in space on the seemingly sensible, but ultimately unworkable and factually unsupportable, view [1] that all such attenuated expressions cause an “initial interest”; [2] that such interest must rise to the level of “initial interest confusion” prior to the point of sale; and [3] 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.\(^{120}\)

Subsequent commentators include a few who have endorsed,\(^{121}\) and many who have criticized,\(^{122}\) the so-called Brookfield\(^{123}\) over-protection approach. Subsequent cases, including one in the jurisdiction in which this line of cases arose,\(^{124}\) have backed away from this approach, and it seems to be waning.\(^{125}\) In my prior articles, I have criticized this line of cases for misapplying the doctrine of initial interest confusion in cyberspace insofar as it would make nearly all initial interest actionable and eligible for the full battery of prohibitory trademark infringement remedies. The problem is that prohibitory relief is granted 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

\(^{120}\) Playboy Enters. v. Netscape Commc’ns Corp., 354 F.3d 1020 (9th Cir. 2004); Brookfield Commc’ns, Inc. v. W. Coast Entm’t Corp., 174 F.3d 1036 (9th Cir. 1999); Folsom, Missing the Mark, supra note 9, at 181–96 (selecting these two cases as representative and asserting that both Playboy Enters. 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.

\(^{121}\) See, 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”). He asserts that the initial interest confusion doctrine, properly understood, is the correct way to apply trademark law to metatag and search engine use of trademarks.

\(^{122}\) See, e.g., Zachary J. 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 Communications Corp.: Making Confusion a Requirement for Online Initial Interest Confusion, 20 BERKELEY TECH. L.J. 209, 213 (2005) (stating that Brookfield’s reliance on initial interest confusion is misplaced); Perry Viscounty & Jordan Kushner, Order to Confusion: Trademark Infringement Liability for Search Engine Keying Ads, 1 HASTINGS BUS. L.J. 149, 153, 156 (2005) (explaining that 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).

\(^{123}\) So designated from the case most commonly cited for the doctrine, Brookfield Commc’ns, Inc. v. W. Coast Entm’t Corp., 174 F.3d 1036 (9th Cir. 1999).

\(^{124}\) Playboy Enters., 354 F.3d at 1034 (Berzon, J., concurring).

\(^{125}\) See Folsom, Defining Cyberspace, supra note 8, 110–12 nn.88–91 (observing that the billboard analogy is not only wrong, but exactly backwards).
to remove any underlying focal point harm. At the same time, I have pointed out that there actually might be some cases in which there really is, or at least might very well be, true preclusive-style initial interest confusion in cyberspace. In such cases, trademark infringement by likelihood of confusion may well have been present.

Under-protection and no “use.” It is equally unsurprising that another line of trademark cases, represented by 1-800 Contacts and Holiday Inns, responded by embracing the opposite incorrect 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. In part, this is based on a four-way equivocation of the word “use” in the law of trademarks in ordinary space.

According to the under-protecting view, if the offending actor’s “use” in cyberspace is invisible, unadvertised, not promoted, 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. 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, it is equally unsurprising that another line of trademark cases, represented by 1-800 Contacts and Holiday Inns, responded by embracing the opposite incorrect 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. In part, this is based on a four-way equivocation of the word “use” in the law of trademarks in ordinary space.

According to the under-protecting view, if the offending actor’s “use” in cyberspace is invisible, unadvertised, not promoted, 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. 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, it is equally unsurprising that another line of trademark cases, represented by 1-800 Contacts and Holiday Inns, responded by embracing the opposite incorrect 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. In part, this is based on a four-way equivocation of the word “use” in the law of trademarks in ordinary space.

126. See, e.g., id. at 110–12 nn.91–92 (suggesting that actual preclusive-style initial interest confusion may arise in cases involving actively trapping addresses and in cases involving the photographs of naked models).

127. 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. Id.

128. 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); see also Folsom, Missing the Mark, supra note 9, 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).

129. This characterization is, of course, my own, supported en passant in my prior articles. The cases themselves certainly do not admit to being a novelty. Indeed, in 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. See infra note 134. 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 that explicitly designs law for cyberspace by taking full advantage of the coded nature of that world and the common good that constitutes a discernible basis for developing public policy there.

130. See infra note 145 (describing a four-way equivocation); Folsom, Missing the Mark, supra note 9 at 159–60; Folsom, Space Pirates, supra note 10 at 863 & n.149. I claim that “ordinary” principles of trademark law have never required an offending actor to “use” the offending expression in such a manner as would have created trademark rights in the offending actor (and certainly not in a manner that would yield a specimen sufficient to support a federal trademark registration). All that is required is that the offending actor’s conduct cause a likelihood of confusion with the mark of another, a much lower standard, and one that can be met without any advertising, and without any promotional activity by the offending actor.

131. See infra note 134.
of confusion, then it could follow that none of the offending invisible or attenuated conduct relating to marks in space can possibly constitute trademark infringement. The problem is that such a determination exonerates the actor, even if such conduct not only was intended to cause confusion or deceit but actually does.

Subsequent commentators include some who have endorsed, criticized, or noted the apparent brief ascendency of this “use” requirement or defense. However, more recent cases, including one in the jurisdiction in which this line of cases arose, have backed away from this approach, and they may well signal

132. See Lanham Act, 15 U.S.C. § 1114 (2006) (“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 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); id. § 1125(a) (seemly, for unregistered marks); 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).

133. See Holiday Inns, Inc. v. 800 Reservation, Inc., 86 F.3d 619, 626 (6th Cir. 1996) (reversing judgment notwithstanding trial court’s findings pointing towards actual and intentional confusion).

134. 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, 969–70 (2008) (finding a historical common law formulation and proposing a modern limitation for new technological uses, requiring that: “(1) consumers should be able to perceive the defendant’s application of the allegedly confusing word or symbol; (2) the defendant should closely associate the allegedly confusing word or symbol with goods or services that the defendant is advertising or offering for sale or distribution; and (3) the defendant’s use of the allegedly confusing word or symbol should make a ‘separate commercial impression’ on consumers’); Uli Widmaier, Use, Liability, and the Structure of Trademark Law, 33 HOFSTRA L. REV. 603, 704 (2004) (applauding Holiday Inns as the better approach to the problem: cases like Holiday Inns 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, 1701 (2007) (replying 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”).


136. In the then-current edition of 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 “[t]he balance of scholarly commentary appears to favor a ‘trademark use’ requirement.” GRAEME B. DINWOODIE & MARK D. JANIS, TRADEMARKS AND UNFAIR COMPETITION LAW AND POLICY 472 (2d ed. 2007) (collecting commentators who apparently favor such a requirement).

137. See 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.; see also N. Am. Med. Corp. v. Axiom Worldwide, Inc., 522 F.3d 1211, 1218–20 (11th Cir. 2008) (distinguishing 1-800 Contacts on the basis that
its decline and eventual demise. Some commentators seem to agree that the doctrine is waning, while others offer to mediate the controversy. Others 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 or as unjust enrichment (or restitution), properly understood.

Axiom’s metatag uses resulted in some visual display, and yet going so far as to say: “to 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”).

138. Cases continue to percolate, and the ultimate resolution remains in doubt, but some of the post-Rescuecom trial court decisions that suggest the decline of the separate “use-as-a-mark” requirement for infringement include: Morningware, Inc. v. Heathware Home Prods., 673 F. Supp. 2d 630 (N.D. Ill. 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. Experian Info. Solutions, Inc., 645 F. Supp. 2d 734 (D. Minn. 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. Whether defendants’ sponsored advertisements actually include . . .[the] trademarks in text is not determinative of whether there has been any infringement” and that “the likelihood of confusion turns on the particular circumstances surrounding the manner in which the allegedly infringing website is presented to the consumer”). See also Hamptons Locations, Inc. v. Rubens, 640 F. Supp. 2d 208, 221 n.11 (E.D.N.Y. 2009) (holding there is no “use” requirement under the Anticybersquatting Consumer Protection Act, and suggesting that Rescuecom undermines the premise of 1-800 Contacts even as applied to alleged infringers in Lanham Act trademark cases and so raises the question “whether the definition of ‘use in commerce’ found in § 1127 [of the Lanham Act] should only apply to those portions of the [A]ct prescribing eligibility for registration, and not the sections defining infringing conduct”). If the Second Circuit were to agree that the definition should be so limited, then Rescuecom will have effectively overruled 1-800 Contacts rather than distinguishing it.

139. See generally Margreth Barrett, Internet Trademark Suits and the Demise of “Trademark Use,” 39 U.C. DAVIS L. REV. 371, 373 (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 ‘trademark use’ of the plaintiff’s mark as a prerequisite to infringement . . . liability.”); Michael Grynberg, Things Are Worse Than We Think: Trademark Defenses in a “Formalist” Age, 24 BERKELEY TECH. L.J. 897, 901 (2009) (noting the critiques of trademark law’s expansion, treating the trademark use doctrine as an attempt to fashion a new defense as a check against expansion, but arguing that “efforts to reform trademark law with new defenses lack a firm basis”).

140. Mark P. McKenna, Trademark Use and the Problem of Source, 2009 U. ILL. L. REV. 773, 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 threshold question “put much more weight on that concept than it can bear”).

141. 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).

142. David W. Barnes, Misappropriation of Trademark, 9 N.C. J. L. & TECH. 171 (2008) (proposing a nuanced misappropriation doctrine for application to initial interest confusion on the Internet); see also Lipton, supra note 110 (suggesting a restitutionary doctrine). The trick, of course, is to formulate what, exactly, constitutes a “proper understanding.” I generally agree with these commentators, but I claim that I have better specified the proper application of such principles in the focal point offense, and in the new set of factors for assessing the residual cases of likelihood of confusion by invisible or attenuated uses of trademarked expressions in cyberspace.
In my prior articles, I have criticized the 1-800 Contacts\textsuperscript{143} and Holiday Inns\textsuperscript{144} line of cases and their incorrect “use” requirement. Not only is the “use” requirement a novel and unwarranted reading of equivocal statements in normative trademark law,\textsuperscript{145} it would seem to upset many of its fairly standard applications.\textsuperscript{146} Not only does the unwarranted “use” requirement exonerate predatory, deceptive, and fraudulent conduct, it leaves no other clear common law legal recourse against invisible and attenuated conduct causing a likelihood of confusion (and actual confusion or fraud) in cyberspace.\textsuperscript{147} In its concentration on raising an unnecessary threshold to trademark infringement, it quite overlooks something very like actual fraud or theft, spoilage and invasive conduct. Worst of all, it is inelegant because it is 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. Moreover, the focal point remedy can be limited to reasonable technological accommodations rather than an all-or-nothing prohibitory approach. The trademark “use” defense, considered as a well-intentioned means to prevent the Brookfield-style over-protection of marks in cyberspace and as a check against the overly expansive “initial interest confusion” line of cases following Brookfield, 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.

\begin{enumerate}
\item 1-800 Contacts, Inc. v. WhenU.com, Inc., 414 F.3d 400 (2d Cir. 2005).
\item Holiday Inns, Inc. v. 800 Reservation, Inc., 86 F.3d 619 (6th Cir. 1996).
\item Folsom, Defining Cyberspace, supra note 8, at 159–64 (equivocal uses of the word “use”: [1] a proprietor-side use of a designation “as” a mark sufficient to create trademark rights, [2] a proprietor-side use in interstate or foreign commerce sufficient to support federal Commerce Clause jurisdiction under the Lanham Act, [3] a proprietor-side use evidenced by a tangible specimen of use sufficient to satisfy a trademark office examiner under the standards promulgated by the Patent and Trademark Office for federal registration under the Lanham Act, and [4] a proprietor-side use sufficient to support geographical priority (or, transnationally, to avoid prohibited extra-territorial extension of non-U.S. trademark rights into the United States by constituting some sort of qualifying “use” within the United States) all conflated, and confused with [5] some conduct (a “use” of an expression) by an offending actor that causes a likelihood of confusion).
\item Folsom, Space Pirates, supra note 3, at 865–67 & nn.161–64 (giving 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 conduct: consider instances of false labeling, product substitution, “patch sets” and other common cases). Maybe the patch-set cases were wrongly decided in ordinary space, but they seem to be well-established by now, and “retrading” them sub silentio in cyberspace is not the better way either for designing law in cyberspace or for reforming law in ordinary space.
\item Id. at 857 n.162 (giving examples of conduct that would be exonerated in ordinary space were the “use” requirement of advertising and promotion applied there as rigorously as some propose to apply it in cyberspace). Holiday Inns is an example of a case exonerating intentional and actual confusion in cyberspace.
\end{enumerate}
2. Failed Likelihood of Confusion Factors

Likelihood of confusion and inapt “factors.” 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 incorrectly prohibits nearly “all” attenuated uses, but also reject the *Holiday Inns–1-800 Contacts* rule of thumb, which incorrectly 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-style 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.

There is a fundamental problem with actually assessing trademark infringement by likelihood of confusion for invisible, attenuated, or expropriating uses in cyberspace according to the current tests. Once both the alternative, over-protecting or under-protecting, gatekeeper rules are gone, there will be no simple trademark heuristic for prohibiting or exonerating every use in cyberspace. Rather, each case will have to be assessed against some meaningful set of factors. From the perspective of current trademark law, this problem is even more difficult than the innovative, well-intentioned, but incorrect rules of thumb just discussed and dismissed. This is because the current factors for assessing likelihood of confusion are inapt when applied to dynamic focal points.

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 *Polaroid* factors under the assumption that some, but not all “uses” of an invisible or attenuated mark in cyberspace constitute trademark infringement. Under this assumption, some of those are legitimate uses of a focal point and others constitute actionable wrongs. The problem is that the current tests cannot reliably predict which are which.

The last problem for trademark law is at least as great as the first set of problems (the gateway problems of “initial interest” and of “use”). The last problem is the failure in cyberspace of the ordinary *Polaroid* factors themselves. Those factors are eight: (1) strength of the mark; (2) degree of similarity between

---

148. See supra notes 120, 143–147 and accompanying text (summarizing my views).
149. *Brookfield Commc'ns, Inc. v. W. Coast Entm't Corp.*, 174 F.3d 1036 (9th Cir. 1999).
150. See infra notes 155–175 and accompanying text (exploring the difficulties of applying existing factors).
The expressions; (3) proximity of the products; (4) likelihood the proprietor will bridge the gap; (5) actual confusion; (6) intent (reciprocal of defendant’s bad faith); (7) quality of the defendant’s product; and (8) sophistication of the buyers. They may work well enough in ordinary space or anywhere else that a juridical agent already knows, or might be guided by common sense, common experience, and practice towards the “right” answer apart from applying any of the factors. Yet, these factors do not work in cyberspace, and common experience is apparently not yet a sufficient guide.

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 factors in the context of cyberspace:

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 that process them. The nonhuman 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. In effect, it makes every mark a strong mark and it entirely ignores the reality of legitimate cyberspace navigation by way of nominative focal points.

---

152. Polaroid, 287 F.2d at 495.
153. See infra notes 154–175 and accompanying text (exploring the difficulties of applying existing factors).
154. Polaroid, 287 F.2d at 495. I use Polaroid only because it is well known. Any of the other circuit court tests could be substituted to the same effect. See generally RESTATEMENT (THIRD) OF UNFAIR COMPETITION §§ 21, 22–23 (1995).
155. Polaroid, 287 F.2d at 495; see RESTATEMENT § 21(d) & 21 cmt. i (discussing the distinctiveness or “strength” of marks).
156. 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). Id. at 408–09. The registered mark included not only a word, but also a design and other elements, and it would certainly seem that the word (apart from the design) was not distinctive, and yet only the word was incorporated in the offending expression. Id.
157. 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. Id. at 1062, 1066.
158. 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. Id. at 1025–26. It would seem “playboy” is no stronger or weaker than “contacts” when it comes to attracting a search engine.
2. Degree of similarity between expressions\(^{159}\): this factor is leveled because all focal points are, by definition, 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 focal point 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\(^ {160}\)—then the inherent hobbling and nullification of these factors necessarily ham-strings any such “knock-out” heuristic.

3. Proximity of products\(^ {161}\): this factor is irrelevant to the focal point problem because regardless of whether the products are the same, related,\(^ {162}\) or wholly unrelated,\(^ {163}\) 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 simply inherent in the nature of commercial markers: expressions that draw traffic to a competitor. The positive inference from products that are wholly unrelated is inherent in the nature of any magnet and any spoiler: expressions that attract, block, hinder, or detour. Neither of these positive inferences, without more, can identify whether there is a likelihood of confusion arising from the focal point expression. Moreover, because commercial markers offering products for sale do not exhaust the category of focal-point abuses, but leave the cases of noncommercial markers and all spoilers untouched, the simple negative inference from a

\(^{159}\) Polaroid, 287 F.2d at 495; see also RESTATEMENT § 21(a) & cmts. c–f (discussing the comparison of designations).

\(^{160}\) See Barton Beebe, An Empirical Study of the Multifactor Tests for Trademark Infringement, 94 CALIF. L. REV. 1581, 1582, 1623–26 (2006) (drawing upon data for a five-year period and concluding the data shows that nonsimilarity is a dispositive factor).

\(^{161}\) Polaroid, 287 F.2d at 495; see also RESTATEMENT § 21 (e), cmt. j (discussing the competitive proximity of the products).

\(^{162}\) The products might be related as competitive, substitutional, or complementary. The corresponding focal points 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.

\(^{163}\) A dynamic focal point coupled to an unrelated product might still trap, capture, disrupt, or spoil navigation tied to the intended focal point.
noncompeting marker is not dispositive. All this is to say, there is no necessary inference that a person using a focal point as a commercial (or noncommercial) marker or magnet 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 treading (or trading) on anyone’s goodwill. This factor becomes useless, thus irrelevant.

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 the world of “cyberspace.” In flirting with this second sense of the concept, it must be that we are asking this question as if it were either a matter of geographic priority or of media priority. It is as if ordinary space were like Kansas and cyberspace were like Nebraska. Or it is as if ordinary space were like radio, newspaper, or billboard, and cyberspace were like television or posters on the sides of buses (a distinction that wouldn’t make a difference in ordinary space). 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 the face of the “good-faith” remote geographic user standard for the second user in virtual geographic places.

5. Actual confusion: this factor 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 reasonable consumers, some plurality of whom may be quite happy to make nominative use of focal points to browse cyberspace without suffering any likely confusion whatsoever, and yet another plurality, some of whom might be situationally bewildered or ambushed by uninvited or invasive interventions, and who might be confused. And then the problem is redoubled by the shifting, sequential, and more or less vulnerable roles any user might from time to time inhabit. In contrast, one benefit 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 to reliably measure the user’s actual status in real time and without any need for hindsight reconstruction or statistical modeling of what “might have been likely to have happened.”

6. Intent (“reciprocal of the defendant’s good faith in adopting the offending expression”)\(^\text{171}\): 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 cause a likelihood of confusion by doing so, but the point of the limited common remedy for the parallel focal point offense is to ensure that the focal point offense is remediated by a reasonable technological accommodation without regard to intent to draw or block traffic. Instead of “intent” to draw traffic, the very fact and nature of the “polling” (or request for accommodation sought by the offended party), followed by a reasonable technological accommodation or a refusal to accommodate, should serve as a better proxy for good or bad faith. Refusal to accommodate would be a more meaningful indicator than simple “intent.” In this respect, there is a good match between the predictive value of “bad faith” in ordinary space\(^\text{172}\) and the deliberate refusal voluntarily to provide reasonable technological accommodations in cyberspace. The advantage to the new factor is

---

169. See infra note 248 and accompanying text for “polling” as part of my proposed new factor analysis.
170. The contrast between my proposed new/transformed factors and old factors helps to illuminate the difficulties of the old factors. See infra text accompanying notes 215–225 (setting forth the new test).
171. Polaroid, 287 F.2d at 495; RESTATEMENT § 22.
2012 / Poisoned Flowers, Part 1

the ability to reliably test by the technique of sampling or polling at the point of the contested action.\textsuperscript{173}

7. Quality of the defendant’s product\textsuperscript{174}: this is an idiosyncratic, if not erroneous factor in ordinary space and is no more conclusive in cyberspace.

8. Sophistication of the buyers\textsuperscript{175}: this factor is not helpful in assessing the problem in cyberspace because spoofing or ambushing, and spoilage or waste may very well have their effect regardless of sophistication. The potentially 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 nor is there any singular “ordinary consumer.” Accordingly, this is a factor with limited inference confidence.

In cyberspace, these traditional factors provide false positives, fail to filter or distinguish, and are often irrelevant, unhelpful, and unreliable, leading to noncogent inferences on the ultimate question of likelihood of confusion caused by invisible or attenuated uses.\textsuperscript{176} 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,\textsuperscript{177} or that some modest additions to or fine-tuning of the factors

\textsuperscript{173} 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 test for likelihood of confusion arising out of new technological uses is set forth infra in the text accompanying notes 215–225.

\textsuperscript{174} \textit{Polaroid}, 287 F.2d at 495; see RESTATEMENT § 21(e) & 21 cmt. k (discussing how markedly different quality may suggest different purchasers or different market channels, or products otherwise unlikely to be associated with a common source, but concluding that evidence of inferior quality “is more properly relevant to fashioning appropriate relief if a likelihood of confusion is otherwise established”).

\textsuperscript{175} \textit{Polaroid}, 287 F.2d at 495; see generally RESTATEMENT § 21(c) & 21 cmt. h (discussing the “care exercised by purchasers” in combination with their buying habits as constituting factors that “can be important”).

\textsuperscript{176} See supra notes 155–175 and accompanying text.

\textsuperscript{177} But see, e.g., Stacey L. Dogan & Mark A. Lemley, \textit{Trademarks and Consumer Search Costs on the Internet}, 41 HOU. 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. Frisch, \textit{Searching for Initial Interest Confusion and Trademark Protection in Cyberspace}, 6 U. PITT. J. TECH. L. & POL’Y 4 (2005); Daniel C. Glazer & Dev R. Dhamija, \textit{Revisiting Initial Interest Confusion on the Internet}, 95 TRADEMARK REP. 952, 953 (2005); David M. Klein & Daniel C. Glazer, \textit{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).
might do the trick. The factors just do not work very well because they are ill-adapted to uses that are invisible to consumers and are often untethered from any directly observable 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, such as 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 far better simply to add a new set of factors for cyberspace. My proposal does just that: instead of glossing the old, it adds a new analysis, applying it only when the “place” of use is cyberspace and the “nature” of use is exceptional because of the power of code. The new analysis, 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 isolates the solution to the special problems in the coded world of cyberspace, and it avoids inadvertent doctrinal creep back from cyberspace into 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”

178. But see Eric Goldman, Deregulating Relevancy in Internet Trademark Law, 54 EMORY L.J. 507, 584–85, 596 (2005) (proposing a new factor, relevancy, designed to weigh the surfer’s intent when using the expression with the goal to deregulate keyword use by search engines to ensure that the prime purpose of the Internet—obtaining information—will not be needlessly shackled); Adam Silberlight, Comment, www.How to Be a Master of Your Domain.com: A Look at the Assignment of Internet Domain Names Under Federal Trademark Laws, Federal Case Law and Beyond, 10 ALB. L.J. SCI. & TECH. 229, 278–79 (2000) (proposing a new factor: “the amount of foreseeable number of hits a web site is likely to get”).

179. 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, since there is one, by an explicit critique of the existing factor tests. See infra notes 154–175 and accompanying text (exploring the difficulties of applying existing factors). One thing missing from most cases is any factor analysis that is dependent on forensically available facts (that is, facts of the sort that might be efficiently collected and rationally assessed to determine likelihood of confusion without recourse to ipse dixit conclusions or question-begging analyses). Better designed factors would better focus the inquiry.

180. See Stephan Miller, A Management Philosopher with Heady Ideas About Beer, WALL ST. J., Nov. 11, 2009, at A18, available at http://online.wsj.com/article/SB125789690177942463.html?mod=googlenews-wsj (on file with the McGeorge Law Review) (quoting the management theorist, Russell Ackoff: “All of our social problems arise out of doing the wrong things righter. The more efficient you are at 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!”).
2012 / Poisoned Flowers, Part 1

controversy and the “use as” controversy in cyberspace. Both of these are 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. Instead, I previously proposed a robust new analysis, “the nature and place of use,” that can be adapted to trademark likelihood of confusion and that can specify a new set of factors for resolving trademark infringement by invisible and attenuated uses of expressions in cyberspace that incorporate trademarks.

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.

181. “Orthogonal” in this context has finally made its way to the Supreme Court 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: I’m sorry. Entirely what?


CHIEF JUSTICE ROBERTS: Oh.

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

MR. FRIEDMAN: Orthogonal.

JUSTICE SCALIA: Orthogonal.

MR. FRIEDMAN: Right, right.

JUSTICE SCALIA: Ooh.

(Laughter.)

JUSTICE KENNEDY: I knew this case presented us a problem.

(Laughter.)

MR. FRIEDMAN: I should have—I probably should have said—

JUSTICE SCALIA: I think we should use that in the opinion.

(Laughter.)

. . .

CHIEF JUSTICE ROBERTS: Or the dissent.

(Laughter.)

MR. FRIEDMAN: That is a bit of—a bit of professorship creeping in, I suppose.


182. Folsom, Space Pirates supra note 3. The new “nature and place of use” factors for testing likelihood of confusion are repeated in this article. See infra notes 215–267 and accompanying text.
3. The Real Problem—Focal Points in an Objective Cyberspace

The problem is dynamic focal points. The best and most efficient of them contain trademarked expressions. Some uses are helpful to the goals of access, navigation, and information-activity, and provide trustworthy markers to vulnerable augmented presences (users) by constructing or supporting a virtual map to cyberspace. Other uses are predatory, invasive, uninvited, and destructive of the map—they spoil, waste, expropriate, or otherwise wreck cyberspace in an objective manner that leaves a trace. These are not necessarily trademark problems at all. They are focal point problems.

Some focal points contain trademarks. These constitute new technological uses, but certainly count as a “use” that might cause a likelihood of confusion. It would be bad law, bad policy, and bad for cyberspace navigation itself to prohibit all new technological uses, because a blanket prohibition would prohibit value-added mapping and would increase search costs without weighing the costs against the benefits—not everything that creates an “initial interest” causes any likelihood of confusion. It follows that if neither none nor all uses of focal points containing trademarks cause a likelihood of confusion, some uses do. The problem is to distinguish one from the other.

It is time now to proceed to the next part of this article. Granting the necessity of specifying a new rule regulating focal point offenses, and the need for revising trademark law to accommodate the new phenomena, can these things be done? I claim they can.

III. RESOLVING THE PROBLEMS: THE NATURE AND PLACE OF USE IN THE CODE WORLD

A. The Focal Point Offense

My threshold claim is that the focal point offense can be specified. I further claim in a forthcoming article that the focal point solution works much more easily than any competing model, its benefits greatly exceed the costs of implementation, it is clearly permissible under existing principles of law, and it ought to be adopted. This article simply explains the threshold claim. I describe the new focal point offense in rule-specific form, relating it to a specified and complementary set of factors for trademark’s likelihood of confusion analysis, coupled with a common and limited remedy and principles for managing secondary liability. 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
2012 / Poisoned Flowers, Part 1

complicated by disconcerting anomalies and in need of replacement. In this section, I set forth the specified focal point offense.

All of this is part of a larger “nature and place of use” analysis for recognizing unique problems in the code world, specifying a solution, and designing a coded resolution that adjusts laws, norms, prices, and architecture to meet the specification.

1. Deliberate Misuse of Focal Points

I claim that the deliberate misuse of focal points in cyberspace constitutes an actionable form of misrepresentation (or fraud), misappropriation (or theft), spoilage, or unfair competition (and, in some cases, unjust enrichment). This result follows under either (a) ordinary principles of law as developed in “ordinary space” and more or less directly transposed, mutatis mutandis, to cyberspace or (b) 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 cyberspace offenses is a step toward creating a law purposely designed for cyberspace, and intended to influence the architecture of the code world. These offenses are characterized by an abuse of dynamic focal points in cyberspace.

A focal point offense comprises deliberate and calculated deception, misappropriation, waste, or unfair competition in an objective cyberspace that 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 routinely occur 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 and definitions.

183. 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 (2d 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.”).

184. See, e.g., Folsom, Space Pirates, supra note 3, at 912 (glossing new terms in an appendix).
2. The Rule-Specific Definition of the Focal Point Offense

There are focal points, dynamic focal points, and dynamic focal points that incorporate someone else’s trademark. We are already familiar with focal points in ordinary space, such 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 device, to deliver an augmented presence to a location. Let us recognize that dynamic focal points can be (1) “inherent” or (2) “associative.”

Inherent focal points include expressions such as “Eiffel Tower,” which do not include any trademark. Among those that are associative are any arising from associated information, with or without a trademark, perhaps including the one particular restaurant in Paris where we have met before. Among associative focal points, perhaps the most powerful and most generally known associations are those that incorporate the trademark of another person. Existing trademark law is ill-equipped to handle the problem of dynamic focal points that incorporate trademarks as associative focal points.

---

185. A focal point has psychological salience. See supra note 43 and accompanying text.
186. 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.
187. Taking an example from the telephone side of cyberspace, a dynamic focal point that incorporates a trademark is “1-800-HOLIDAY” or, more generally, any phone number in the form “1-nnn-TRDMARK.” On the Internet side, a dynamic focal point that incorporates a trademark is “PANAVISION.com” or any address in the form “nnnTRADEMARKnnn.com.” Instead of “.com” the formative might be “.org,” “.net,” “.edu,” or any other now- or later-approved global top-level domain (gTLD), or it might be “.nu,” “.tv,” or any other catchy country code. Or more generally, it might be any other high-level (natural) or low-level (machine) language, code, or convention for creating or pointing to locations in space—my approach is not tied to any particular technique by which a focal point might be embodied.
188. See supra note 44 and accompanying text.
189. See id. (noting that the Eiffel Tower is an inherent focal point).
190. 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.
191. 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,” RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 9 (1995), it follows that every trademark is an associative focal point (though not every associative focal point is a trademark).
192. 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 for 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 supra Part II.D (“when trademark fails”).
2012 / Poisoned Flowers, Part 1

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

In an objective cyberspace that relies upon a virtual map featuring dynamically coded focal points functioning as markers and spoilers (addresses, magnets, roadblocks, or detours), any [conduct]/[new technological use] that hinders or prevents robust access of, or reliable navigation to, retrievable and active information, including conduct that:

(a) alters the map (“tampers”);\footnote{193}

(b) plants deceptive focal points (“spoofs”);\footnote{194}

(c) ambushes a user of focal points with uninvited, invasive, or false invitations (“ensnares”);\footnote{195} or

(d) expropriates, blocks, or wastes focal points otherwise available (“spoils”);\footnote{196}

classifies as a focal point offense, subject to the limited common remedy.

It should be understood that “conduct” is a term that includes any new technological use of a trademarked expression,\footnote{197} but is designed to free the focal point offense of the baggage that has accumulated around the trademark “use-in-cyberspace” controversy. My proposed language embraces either terminology.

\footnote{193. 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.}

\footnote{194. 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 mimicked 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.}

\footnote{195. An actor ambushes a user by catching a user off-guard, intercepting the user’s communications, invading the user’s privacy, or otherwise trapping, misdirecting, or misleading augmented presences, providing unasked-for information, or deluging a user with chaff thereby frustrating navigation.}

\footnote{196. An actor spoils a focal point by taking a focal point out of circulation, expropriating associative focal points that are associated with another person, place, or community of interest, or 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.}

\footnote{197. See infra text accompanying note 204 (defining “use” and “new technological use” for purposes of trademark analysis of focal point offenses that happen to incorporate a trademarked expression).}
Perhaps of more fundamental importance, I am proposing no individual private ownership of, nor property in, any focal point, but rather I am proposing harm-based, liability-style rules tied to specific offenses. These offenses sound in misrepresentation and fraud, misappropriation and theft, waste and spoilage (and, in some cases, unjust enrichment), all as examples of a particularized and specified development of common law doctrines of tort and unfair competition, passing off, and trademark (or restitutionary) antecedents, deliberately adapted to the felt needs of an objective cyberspace.

3. Limitations and Integration

The limited remedy is integral to the offense and is essential to understanding that the focal point offense is modest. 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. The limited remedy applies only as and to the extent necessary, and only after request. Thus, it will not encumber cyberspace with extraneous and clumsy regulation. Secondary liability is also controlled and limited. I discuss these features in Parts III.C.2 and 3 of this article.

B. Trademark Law Revised for Attenuated and Invisible Uses

I have already demonstrated that the recently debated gatekeeping rules fail to work. Therefore, the threshold questions of “use” and “initial interest” are my first revisions to existing trademark law. I have also demonstrated that current likelihood of confusion factors are inapt when applied to invisible and attenuated uses. Accordingly, the substantive factors for “likelihood of confusion” are my next revisions to existing trademark law when dealing with attenuated and invisible uses. These discussions follow in the next parts of this article.

198. The characteristics of an objective cyberspace have been discussed. See supra Part II.B.2.
199. The limited remedy is discussed at Part III.C.2. 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.
200. 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.
201. See supra Part II.D.1.
202. See supra Part II.D.2.
2012 / Poisoned Flowers, Part 1

1. Threshold Questions: “Use” and “Initial Interest”

Once the gatekeeping rules are down, it is necessary to reconsider “use” and “initial interest” more realistically.

New Technological Uses in Cyberspace. The answer to the question whether trademark 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, and reject in trademark analysis any nascent White-Smith bias. 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 technological uses in trademark law, avoids ducking the issue, and is appropriate for trademark law in the code world:

Any [new technological use] / [invisible, attenuated, or expropriating use in cyberspace] 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, constitutes a “use” which might cause a likelihood of confusion of source, sponsorship, or affiliation (including by interfering, tampering, spoofing, ambushing, or spoiling) if in connection with, or interfering with, marketing goods or services in commerce. A “new technological use” [or invisible, attenuated, or expropriating use] includes any conduct by an actor in connection with any coded expression in cyberspace. It 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 or that makes any directly observable tie to any particular product, and it need not make any separate commercial impression on a consumer. If the use is no more than an invisible or attenuated use, liability is limited to the common remedy.

203. White-Smith Music Publ’g Co. v. Apollo Co., 209 U.S. 1, 17 (1908); see also supra notes 54–55 and accompanying text (discussing what I and others refer to as the White-Smith anti-technology bias in copyright law).

204. The first sentence is modeled in part on the copyright solution: “Copyright protection 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, 17 U.S.C. § 102(a) (2010). The following sentences specify 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.
Limitations against over-protection of marks in cyberspace are no longer found in the definition of “use,” but are built into (a) the newly specified focal point offense and the new likelihood of confusion analysis for residual trademark infringement cases, coupled with (b) the limited common remedy that is not only part of the new focal point offense, but is also incorporated into the correspondingly transformed likelihood of confusion analysis. There is no need for artificial and anti-technologically biased barriers at the threshold “use” level prior to beginning the trademark infringement analysis. The bracketed language permits alternative phrasing (and updates the “invisible, attenuated, and expropriating use” language I had used in prior articles to the simpler and more generalized expression, “new technological use,” that I propose here).

Initial Interest. The answer to the question, whether dynamic focal points incorporating trademarks should raise concerns of initial interest confusion in cyberspace, should parallel the answer originally formulated for initial interest confusion in ordinary space, in light of the reasons for the rule. It should also be consistent with the revised trademark likelihood of confusion factors for invisible and attenuated uses. Thus:

“Initial interest” by [a new technological use or] an invisible, attenuated, or expropriating use in cyberspace that does not otherwise cause a likelihood of confusion with the mark of another under the ordinary rules governing likelihood of confusion in ordinary space at the point of sale may be actionable if [(a) it causes likelihood of confusion under the rules governing new technological uses or invisible, attenuated, or expropriating uses in cyberspace or (b)] it precludes fair consideration of the other’s goods or services.

The first bracketed expression updates the “invisible, attenuated, or expropriating use” expression I introduced in prior articles to the “new technological use” language I propose here. The second bracketed expression refers to the proposed rules for likelihood of confusion set forth in Part III.B.2, which is the section immediately following this one. For ease of discussion, I refer to the distinctive residue as “preclusive-style” initial interest confusion in cyberspace. I propose that not every case of initial interest should be actionable. That would be far too broad and would run the risk of prohibiting value-adding navigational markers, which reduce search costs and almost certainly do not cause any realistic likelihood of confusion to any substantial number of reasonable consumers in cyberspace. Instead, only those cases of preclusive-style initial interest ought to be screened for likelihood of confusion based on initial
interest. I have previously discussed issues with the likelihood of confusion factors in ordinary space, and in their point-of-sale context, in a prior article:\(^\text{205}\):

One peculiarity [of likelihood of confusion in ordinary space] is this: likelihood of confusion is usually assessed at the point of sale, but sometimes before.\(^\text{206}\) This temporal disruption can lead to a finding of likelihood of confusion (prior to sale) in the absence of any possible confusion whatsoever (at the time of sale).\(^\text{207}\) This, in turn is complicated by disclaimers that sometimes suffice to dispel any confusion (at the point of sale) but at other times fail to dispel confusion.\(^\text{208}\) A presale problem gives rise to what is called “initial interest confusion”—the actionable harm to the proprietor of the mark occurs if, because of likely confusion prior to the point of sale, the proprietor ‘may be precluded from further consideration by the potential purchaser in reaching his or her buying decision.’\(^\text{209}\) Initial interest confusion might seem very like a finding of trademark infringement liability in the absence of likelihood of confusion, but [when preclusion is added, the doctrine’s] rationale is in fact based on a temporal likelihood of confusion (presale) that likely deprives the mark proprietor of a potential customer (at the point of sale).\(^\text{210}\) The problem with point of sale disclaimers in ordinary space is that, even though they may be clearly worded, it is not so clear whether they are effective.\(^\text{211}\) Sometimes disclaimers are sufficient, sometimes not, depending on the circumstances.\(^\text{212}\)

\(^{205}\) Folsom, Missing the Mark, supra note 9, at 155–56.

\(^{206}\) See 3 J. Thomas McCarthy, McCarthy on Trademarks and Unfair Competition \S 23.01[4][b] (3d ed. 1996) (presale) (selecting this edition to gauge the law as understood circa 1996, prior to the 1999 decision in Brookfield). There may be liability for confusion after the point of sale as well, id. \S 23.01[4][c] (post sale), but such “post-sale” confusion does not presently pose the same problem for invisible and attenuated uses in cyberspace as does “pre-sale” (or “initial interest”) confusion.

\(^{207}\) See id. \S 23.01[4][b].


\(^{209}\) 3 McCarthy, supra note 206, \S 23.01[4][b] (emphasis added) (quoting HRL Assocs., Inc. v. Weiss Assocs., Inc., 12 U.S.P.Q.2d 1819 (Trademark Tr. & App. Bd. 1989) (determining that initial interest confusion constitutes a ground to deny registration under Lanham Act \S 2(d) in a PTO inter partes proceeding, and that injury to the proprietor of the mark occurs “if a potential purchaser is initially confused between the parties respective marks in that [the proprietor] may be precluded from further consideration by the potential purchaser in reaching his or her buying decision.” (emphasis added)), aff’d on other grounds, 902 F.2d 1546 (Fed. Cir. 1990)); Mobil Oil Corp. v. Pegasus Petroleum Corp., 818 F.2d 254, 259 (2d Cir. 1987) (finding liability even though any confusion between “Pegasus” and Mobil Oil’s “flying horse” would be dispelled prior to sale, and the purchaser entered into a business transaction in an unconfused state of mind).

\(^{210}\) 3 McCarthy, supra note 206, \S 23.01[4][b].

\(^{211}\) See Schechter & Thomas, supra note 208, at 649. As a result, while courts “naturally will consider” any disclaimer when analyzing the likelihood of confusion, “the use of a disclaimer does not provide
The ground shifts dramatically in cyberspace. Preclusion is probably rare because a back-click and a reentry is usually an easy thing. Disclaimers, especially of the type I propose as part of the technologically reasonable remedy, almost certainly can be effective in cyberspace because they can truly level the playing field and forfeit the momentary advantage enjoyed by the nonproprietor. Accordingly, true preclusive-style initial interest is ordinarily not the typical situation in cyberspace. Hence there is no place for a nearly conclusive presumption as in *Brookfield*. But neither is there any occasion completely to reject the notion, because at least with what might be called a “sticky” offending use, true preclusion might arise. Finally, as indicated by the bracketed language in the black letter statement of the initial interest rule, the whole issue might be subsumed under (and largely obviated by) the revised likelihood of confusion factors for invisible and attenuated uses, which is the trademark equivalent of the focal point analysis. The discussion of those factors follows in the next section.

2. Likelihood of Confusion

Since some invisible and attenuated uses in cyberspace constitute “use” which might give rise to a likelihood of confusion, and since not all such uses amount to near-conclusive initial interest confusion, it becomes necessary to consider what, exactly, could demonstrate a likelihood of confusion in cyberspace. Once the failed likelihood of confusion factors are rejected, it is necessary to provide a more realistic factor analysis.

My prior articles claim a new “nature and place of use” analysis can resolve the characteristic problems of invisible and attenuated trademark infringement by rationally assessing likelihood of confusion in cyberspace. I can now place that trademark solution in a wider context. Ideally, it is for the residual set of invisible or attenuated use cases not covered by the focal point offense or for which the focal point offense is insufficient. Of course, until such time (if any) as a court or legislative body actually embraces the focal point offense, the “nature and place a ‘safe harbor’” especially when the disclaimer is small, inconspicuous, or not clearly worded. Id.; see Jacob Jacoby & George J. Szybillo, *Why Disclaimers Fail*, 84 TRADEMARK REP. 224 passim (1994) (presenting empirical evidence that many disclaimers are ineffective).

212. Folsom, *Missing the Mark*, supra note 9, at 155–56; see also id. at 157 n.77 (questioning the categorization of the doctrine in ordinary space: the absence of likelihood of confusion at the point of sale makes it seem more nearly a quasi-fraud or quasi-theft phenomena).

213. See generally Folsom, *Defining Cyberspace*, supra note 8, text accompanying note 17 (giving two examples in which possible preclusive-style initial interest confusion might actually occur in connection with invisible or attenuated uses in cyberspace, one having to do with the goods or services associated with the Playboy mark in which the consumer might be completely satisfied prior to leaving the offending site if visual goods were displayed there, and the other having to do with an active sales agent at the offending location competing with Holiday Inns and perhaps convincing the user not to back out of the offending site). There may be other circumstances of sticky sites in cyberspace where preclusive-style initial interest might occur.

214. See generally Folsom, *Defining Cyberspace*, supra note 8 (describing this new analysis).
“of use” analysis, adapted for trademark likelihood of confusion, will be the only common law mechanism for regulating such conduct. Therefore, practically, it may serve on an interim or transitional basis as a way of resolving all invisible and attenuated use cases under an explicitly trademark rubric until the more comprehensive focal point offense is adopted and fully implemented.

In the wider context I am proposing, courts can tailor the new nature and place of use analysis to complement the focal point offense. The identical principle can generate a separate but related trademark-style rule. This is because it can be refocused and fully specified for rule-based application to test for likelihood of confusion for the paradigmatic cases of invisible and attenuated uses of marks in space under a trademark infringement rubric. Here is the rule-specified application of the analysis, in the form of likelihood of confusion factors appropriate for invisible and attenuated uses:

> Whether a new technological use [or 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 new technological use [or cyberspace intervention], including the nature of the offending party and the nature of the supposed victim or pseudo-victim, and other persons affected;

(b) the place of use and the degree it implicates foundational cyberspace values;

215. Folsom, Space Pirates, supra note 3.

216. The “new technological use” is defined in Part III.B.1, supra. In my prior article, I capture the same concept by the expression, “invisible or attenuated cyberspace intervention.” Folsom, Space Pirates, supra note 3. Such an intervention is essentially synonymous with “new technological use” as defined herein. I tended to use the “intervention” language in my Space Pirates piece in part to avoid the distraction of the use-as-a-mark controversy by not “using” the equivocal word “use” in the operative phrase. I tend to employ the “new technological use” language now (in part, more directly to confront the use-as-a-mark issue when it comes to new technological uses). From my perspective, the expressions are interchangeable. Each has to do with conduct that causes a problem. The conduct has to do with “using” an expression in a specified way.

217. The intervention might be invited or uninvited; free-riding or value-adding; helpful, harmless, or predatory.

218. The offending party might be a mapper or trapper, surfer or spoofer, resource provider (hitchhiker’s guide) or pirate, advertiser or shill, arbitrageur or aggregator, a competitor, or a provider of an information location or community of interest.

219. The victim (or pseudo-victim) or other person affected might be a surfer, hitchhiker, shopper, consumer (in a search mode), customer (in a purchasing mode), mark proprietor, or resource provider.

220. The place might be cyberspace but it might involve only an ordinary (first-order) transaction transposed from 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 (second-order) transactions not possible at all or only vaguely conceivable in ordinary space.
(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 interference by 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.

The fully specified likelihood of confusion factors recapture, in element (e), a concern for the public interest in navigating cyberspace, and the factors expressly incorporate a limited, graduated, and proportional remedy that takes the public interest into account for purposes of assessing potential trademark infringement or cognate offenses. The new mode of analysis is stated in a rule-specific form, definite enough for ex ante planning, ex post adjudication, and all points in between.

221. 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 notes 257–260 (providing references). 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.

222. See infra note 248 and accompanying text (providing further details); and see Folsom, Space Pirates, supra note 3, 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 11, at 94–100 (extending the analysis and recommending a form of polling, by tendering an offer for a reasonable technological accommodation, as a highly relevant factor in deciding whether to impose secondary liability arising out of new technological uses).

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

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

225. The United States Supreme Court has recently reminded lower 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, 391–94 (2006).
Perhaps equally, if not more significant, is the 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. Does a focal 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 articulating and distinguishing the new focal point offense, together with a purposefully designed “nature and place of use” analysis for likelihood of confusion, is the recovery of the rational factual inquiry that has long been part of any adjudication of liability predicated upon a rule of law.

3. Limitations and Integration

There are some comprehensive common elements essential to understanding the new trademark analysis. The “nature and place of use” is confined to the code world that spawned the problem of invisible and attenuated uses in the first place and is not intended unintentionally to migrate or accidentally to “evolve” into a rule for ordinary space. The analysis is flexible and adaptive. The nature and

226. See generally Dinwoodie & Janis, Lessons from the Trademark Use Debate, supra note 135; see also supra note 179 (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, Trademarks and Competition: The Recent History, 59 LAW & CONTEMP. PROBS. 13, 28 (1996) (“However, because such decisions [assessing likelihood of confusion and assessing validity/distinctiveness] concentrate so heavily on the facts of a particular case, and because this legal doctrine tends to become formalistic and conceptualistic, there is much room for judicial discretion.”), noted in Graeme B. Dinwoodie, The Death of Ontology: A Teleological Approach to Trademark Law, 84 IOWA L. REV. 611, 650 (1999). It may well be that a legal realist might conclude the disingenuously thin “fact-finding” displayed in many reported trademark-related decisions in cyberspace is simply a cloak for a discretionary growth or abatement of trademark law. See generally Dinwoodie & Janis, Lessons from the Trademark Use Debate, supra note 135. I claim a rule of law is better served if there are actual facts that might be both relevant to the legal inquiry and also possible to obtain and demonstrate at reasonable cost.

227. “Let us prepare to grapple with the ineffable itself, and see if we may not eff it after all.” DOUGLAS ADAMS, DIRK GENTLY’S HOLISTIC DETECTIVE AGENCY 188 (1987). It may very well be time, finally, to “eff” the ineffable and to designate some factors appropriate for cyberspace which are actually susceptible of real proof, rather than errant speculation.

228. See supra Part III.B.2 (solving the inapt application of current likelihood of confusion factors as one additional advantage of the “nature and place of use” factor).

229. 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. It encourages law that is deliberately designed by a juridical agent, rather than law that accidentally happens to evolve. See supra Part II.B.2.
place of use invites an extended consideration of typical or characteristic users. The limited remedy, and especially polling to glean highly relevant \textit{ex ante} signals of good or bad faith, is integral to the revised trademark infringement analysis and is essential to understanding that the resolution of invisible and attenuated trademark infringement is modest.\footnote{The limited remedy is discussed at Part III.C.2. 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.} The limited remedy applies only if and to the extent necessary, and only upon request, and so it will not encumber cyberspace with extraneous and clumsy regulation. Finally, an adjustment to secondary liability rules makes sense. These are what I’ve called “third-order” concerns. These unify the focal point offense with the new trademark analysis and are common to both. I treat them in the next part.

\section*{C. Comprehensive Common Elements}

\subsection*{1. Second Order Concerns: Extending the Nature and Place of Use (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, not entirely like those commonly encountered in ordinary space; these present additional second-order concerns in respect of their differences with users in ordinary space. By nature, these users may be (a) invited or uninvited; (b) value-adding or free-riding; and (c) helpful, harmless, or predatory.

These characteristic users can be further identified to include: (1) surfers and mappers (that is, hitchhikers and guides); (2) spoofers and trappers (that is, jokers, pirates, plagiarists and predators); (3) spoilers and arbitrageurs (that is, vandals and economic rent-seekers); (4) shills and advertisers; (5) shoppers and searchers; and (6) consumers, competitors, and mark proprietors. The nature and place of the use of focal points in cyberspace is not an arcane or mysterious thing, but the differences between what happens there and what happens in ordinary space are worth noting.

\textit{Surfers} (leisure-travelers), \textit{searchers} (as generalized seekers or consumers merely “of” information within cyberspace itself), and \textit{shoppers/customers} (persons motivated to shop, by specifically searching for and buying particular branded goods or services) often use focal points to find things. And yet they do so with different interests: perhaps as a motivated shopper looking for a particular brand, a comparison searcher looking for similar products, or a surfer simply looking around. They could be looking for navigational markers out of
mere curiosity (a user as a surfer—a consumer of cyberspace itself), to compare alternative goods or services (a user as a comparison-searcher), or because they specifically want to buy (a user as a customer seeking a particular brand; a motivated-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 who wants to be found in space might 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.

Some of these characteristic users are pirates or plagiarists.231 Again, some of these are targeted defendants, in the sense someone targets them for secondary liability under existing theories of contributory or vicarious responsibility mechanically applied in the code world. Others are opportunistic plaintiffs, in the sense they are attempting to shift the cost of policing their intellectual property to targeted defendants under expansive readings of secondary liability. Finally, others are expected yet often unrepresented “pseudo-victims.”

These pseudo-victims include the vast number of persons who simply want to use cyberspace and whose interests are rarely consulted in current cases. Although they are often assumed to be victims, in many cases they are not, nor has anyone asked them (and they are often harmed, ironically enough, only by the juridically imposed remedies that actually interfere with sensible uses of focal points). The ordinary user, in the capacity of hitchhiker, has an interest in nominative uses of dynamic focal points simply for cyberspace access and

231. Both “pirates” and “plagiarists” have checkered careers in legal discourse, and in my own writing. In this article, I use the terms in contrast to [1] a person who primarily offends against a clearly marked legal rule (i.e., a simple lawbreaker within the territorial jurisdiction of some polity, or in the context of intellectual property, an “infringer” rather than a “pirate” or a “plagiarist”), and to distinguish such lawbreakers and infringers from [2] a person who primarily offends against a moral intuition or against a social norm of a relevant community to which the offender belongs (in the context of an academic community, a “plagiarist”) or [3] a person who transgresses against a well-demarcated but unwritten or extraterritorial rule of law or who wastes, spoils, and vandalizes (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 nonsynonymous meanings to the terms. See infra text accompanying notes 267–269 (discussing “pirates” as a class of persons affected by my proposed new rules).
navigation, and that interest in free access is too often excluded from explicit consideration.

Worse than being excluded, the hitchhiker has sometimes been turned into a pseudo-victim. The result is that the provider of the nominative focal point has occasionally been turned into an actor liable or threatened with liability (directly or indirectly under principles of secondary liability) for initial interest confusion, and hence liable for actionable “likelihood of confusion” under some sort of legal fiction. This is so even where no reasonable hitchhiker is likely to have been confused at all (and is much more likely, in fact, to have benefitted from the use). Likewise, the hitchhiker has an interest in having a reliable hitchhiker’s guide as a resource, and the discussion has neglected the public’s interest in having a reliable map. Finally, if there is to be a hitchhiker’s guide or map, then there might be some cost associated with it. If so, and if the map is a public good, then perhaps someone should be able to prepare a hitchhiker’s guide 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 benchmark “ordinary consumer” for trademark law’s likelihood of confusion test as it has developed in ordinary space. This is why I de-synonymize the “consumer” in cyberspace, and distinguish shoppers/customers and others in a purchasing mode or mood from searchers, hitchhikers, and other users in a surfing mode or mood. It is also why I do the same for the “competitors” and other actors in cyberspace, distinguishing providers of competing goods or services from spoofers, trappers, shills, arbitrageurs and other predators, free-riders, or opportunists; and distinguishing both of these from guides, mappers and other value-adding resource providers, and all in relation to the persons whom they affect. 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

---

232. See supra Part II.B.2 (the place of use: an objective cyberspace).
2012 / Poisoned Flowers, Part I

demonstrates as much or more than any words and better than 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, thereby allowing the law to disarm the one while encouraging the other. When we evaluate the actors according to their conduct, then labels become both meaningful and helpful in resolving disputes—“pirate” becomes more than a meaningless pejorative, and instead signifies an actor engaged in specifically defined predatory conduct.

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 focal points are dynamic, then the “nature and place” of use points to an actionable focal point offense. But the nature and place of use factors also counsel that a specially tailored and proportionate common remedy is in order to fit the remedy to the offense while broadly permitting nominative users of focal points as an aid to access and navigation in cyberspace.

2. Third-Order Adjustments: The Common Remedy

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 prohibitory injunctive relief, so it explicitly embraces the *eBay v. MercExchange* principle of nonautomatic prohibitory injunctions in patent and, by extension, in other intellectual property cases.

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

---

233. 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 note 248 and accompanying text. Sampling or polling is inherent in the focal point offense, and is specified as an explicit factor in the new likelihood of confusion analysis.

234. This is in the spirit of the common aphorism “Factum non verbum” (variously rendered into English, including as “actions, not words”). See, e.g., About TH: General Information, TSINGHUA UNIV., http://www.tsinghua.edu.cn/eng/about.jsp?boardid=32&bid2=3201 (last visited Apr. 8, 2010) (on file with the McGeorge Law Review) (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].”).


236. See Folsom, *Embracing eBay*, supra note 11 (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 9, at 157–59; see also RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 35 (1995).
particularized offenses such as dilution offenses and cybersquatting offenses, whether arising under contractually ordered dispute resolution policies or otherwise. Because the remedy is the same and is proportionate in all circumstances, there is both an immediate simplification and clarification of the law, and there is also less pressure upon juridical actors to find the right label or “cause of action.” Here is a description of the common remedy:

The “common remedy” for a focal point offense, or for likelihood of confusion arising out of a new technological use [or invisible, attenuated, or expropriating use] of a trademark in cyberspace includes one or more of a technologically reasonable, and technologically effective:

(a) disclaimer,
(b) notice,
(c) redirect,
(d) forced release.

237. See infra notes 257–260 (providing references to some other offenses outside of trademark law).
238. “The forms of action we have buried, but they still rule us from their graves.” F. W. MAITLAND, THE FORMS OF ACTION AT COMMON LAW 2 (Cambridge 1971) (1909). Who would have thought that when dealing with new technological uses in the code world, in the twenty-first 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.

239. The disclaimer is a statement that the location is not associated with, sponsored by, or affiliated with a mark proprietor.
240. A notice is an expression which includes the address or other addressable location of the mark proprietor(s) or the persons, places, or communities of interest associated with a focal point (there could be more than one). 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 Folsom, Racing the Genie (forthcoming), supra note 6 (solving the Holiday Inns case as a focal point offense, and discussing “notice”).

241. A “redirect” is a coded expression that will point the user to the dynamic location of the mark proprietor, or the most likely proprietor if more than one, or to a person, place, or community of interest associated with a focal point. 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 ‘MOVIEBUFF’ as a trademark for high-end professional-grade databases about motion pictures.” See Folsom, Racing the Genie (forthcoming), supra note 6 (solving the Brookfield case as a focal point offense, and discussing a “redirect”).

242. 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 Folsom, Racing the Genie (forthcoming), supra note 6 (solving the Holiday Inns case, as a focal point offense, and discussing a “forced release”).
2012 / Poisoned Flowers, Part 1

(e) reciprocal auction,\textsuperscript{243} and

(f) opt-out/opt-in.\textsuperscript{244} It may also 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 (this request-response cycle constitutes "polling" or "sampling.")\textsuperscript{246}

The same technology which enables 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.

Reasonable Technological Accommodations. It is important to stress that all I am presently proposing are "reasonable" technological accommodations. Where there is more than one coexisting trademark proprietor or focal point association (more than one person, place, or community of interest), and perhaps a very large number of them, a reasonable remedy for multiple focal point claimants—by notice, redirect, forced release, or auction—may be limited to a subset or a list drawn from the stronger focal point associations, not unlike the permissible sharing of famous marks in ordinary space.\textsuperscript{248} I am not supposing nor proposing

\begin{itemize}
  \item \textsuperscript{243} A "reciprocal auction" might put the associative focal point up for bid to that relatively small set of users who have an association with it, but with the understanding that the "winner" might be expected to include reciprocal cross-notices directing traffic to the "losers" of the auction. For example, "Ford.com" might be auctioned to a group potentially including the Ford Motor Company, the Ford Modeling Agency, the Gerald Ford Presidential Library, or the Ford Theater historic landmark and restoration committee. It might even, conceivably, include various communities of interest within the auction pool: the friends of Ford (some fan club or community of interest), or the enemies of Ford (some anti-fan club or community of interest), though it might seem they would be served by FordRules.com or by FordStinks.com, respectively. One immediate advantage of the proposed solution is that it wrings the opportunity for arbitrage out of the valuation calculation: since the winner will still have to provide a reciprocal disclaimer, notice, redirect, and/or forced release, the spread between cost and price should shrink dramatically. See Folsom, \textit{Racing the Genie} (forthcoming), supra note 6 (solving the arbitrage problems as one additional advantage of the focal point analysis).
  \item \textsuperscript{244} An "opt-out" is a conspicuous offer to a user, by which a user can choose from time to time whether to be a billiard ball in cyberspace (by permitting keystrokes to be intercepted as triggers) or not (by refusing to permit invasive trapping of keystrokes by strangers and predators). See Folsom, \textit{Racing the Genie} (forthcoming), supra note 6 (selectively solving the invasion of privacy problems, while enabling those who welcome such advances, as one additional advantage of the focal point analysis).
  \item \textsuperscript{245} See infra note 248 and accompanying text.
  \item \textsuperscript{246} See supra notes 240–243 (making allowance for the possibility of more than one accommodated party according to a reasonable technological resolution); see also Folsom, \textit{Racing the Genie} (forthcoming), supra note 6 (including examples involving such cases); and cf. generally Robert Brauneis & Paul J. Heald, \textit{Trademark Infringement, Trademark Dilution, and the Decline in Sharing of Famous Brand Names: An Introduction and Empirical Study}, George Washington Univ. Legal Studies Research Paper No. 510 (Aug. 2010) (abstract), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662623 (on file with the \textit{McGeorge Law Review}) (according to an empirical study, sharing of famous marks by multiple users appears to be on the decline: a fifty-four percent drop between 1960 and 2010 in the use of some 131 famous marks by
\end{itemize}
that there is any need to seek the “best” accommodation.\textsuperscript{247} Indeed, the search for the best could be counterproductive, time-consuming, difficult to prove, and quite likely to be outmoded by or shortly after the time it is finally adjudicated. If juridical agents are not to be or become electrical engineers (and they should not), and if they ought not to study the new machines in any excruciating detail, it would seem to follow that they certainly ought not to suppose they can adjudicate the best technology. Recalling that all we need is to recode Martha’s flowers (or Dank’s dog), what we want is something that will impel the parties to do so. If it should be relatively efficient for Martha to recode her flowers, then let her do so. If Martha should be able to demonstrate that it is relatively more efficient for Dank to recode his dog, then let him do so (and let Martha pay for the solution). If the whole enterprise is ridiculously, or merely unreasonably, expensive but Dank were prepared to contribute to the cost, then let that be the solution. There is much more to say about this, but it must await the forthcoming installment. For now it should suffice to say that remediating code is very likely available to counteract offensive code, probably at a reasonable cost, and especially if all the parties know ahead of time that it is the price to be paid for otherwise offensive abuses of focal points.

\textit{Polling.} I include “polling” or “sampling” within the battery of limited remedies. It is more precisely a technique, and an important one, made possible in the code world and potentially dispositive in the context both of focal points and of invisible or attenuated trademark liability. In its ability to capture readily available, highly relevant evidence, “sampling” or “polling” is an especially interesting and important concept,\textsuperscript{248} and one that takes advantage of coded persons other than those that made the marks famous). But while the number is declining, there is still a nonnegligible plurality of coexisting users of famous marks in ordinary space. \textit{Id.} Coexistence of multiple users of common focal points in cyberspace by reasonable technological accommodation should be no less, and probably much more feasible, than coexistence of famous marks in ordinary space. I thank Professor Elizabeth Winston for suggesting the importance of mentioning the multiple-claimant cases in this article, thereby permitting me to add appropriate provisos in notes 240–243, \textit{supra}.

\textsuperscript{247} In this respect, I am proposing a solution at least nominally, and perhaps substantively, different from that of Professors Helman and Parchomovsky. \textit{Cf.} Lital Helman & Gideon Parchomovsky, \textit{The Best Available Technology Standard}, 111 \textit{COLUM. L. REV.} 1194, 1217–19 (2011) (proposing to solve the somewhat analogous problem of secondary copyright liability for webhosts, shielding those from liability who employ the “best” filtering technology available on the market; not “perfect” but “best” in terms of “effectiveness-to-cost” comparisons). I believe the Helman–Parchomovsky “best” may, and certainly will, if that standard should begin to creep towards perfection or to require heroic fact-finding, become an enemy of the good. A “reasonable” technological accommodation is sufficient for my proposal. If a claimant is disappointed because there is another technology that seems better or best, then the claimant may have it if the claimant will offer to pay the difference between it and the “reasonable” accommodation my proposal requires. That is, let the “default” be relatively cheap and easy to find, and let the party most interested buy an adjustment to the default if “better” or “best” is desired, available, and worth the cost. I am as much concerned with potential abuses committed by the opportunistic plaintiff aided and abetted by an overly solicitous judge in ordinary space as with those committed by the offending actor in a coded world, and I propose a balance in order not to load cyberspace with unreasonable and unnecessary burdens.

\textsuperscript{248} “Sampling” or “polling” is inherent in the focal point offense and it is an explicit factor as part of element “d” in the proposed likelihood of confusion test. \textit{See supra} text at note 222 (reciting that element).
responses available in cyberspace. By constructed code, it would be possible to query, sample, or poll 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 code-generated 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” or pseudo-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 persons 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 *ex ante* determination of both subjective intent and objective effect. According to the first and second queries, the offer or refusal to offer such cooperation as requested by the mark proprietor’s “sampling” or “polling” request, and 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 that the only person in Martha’s position who would refuse such cooperating accommodations in the code world 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.

3. **Third-Order Adjustments: Controlling Secondary Liability**

Just as I have written on limited damages elsewhere for brevity here, so also I have written on limited secondary liability for the same reason. I have previously
argued that we would do well to reframe the conditions under which it is ever just to hold another person liable for an actor’s wrongful conduct in ordinary space. I have claimed that we may do so according to articulated criteria:

(1) fault (contributory or inducement-style secondary liability),

(2) status (genuine agency or the special “adjusted for copyright sort of nonagency accompanied by a direct financial interest and an ability to control”),

(3) consent (voluntary surety or guaranty relationships, supplemented by the rules of law that tend to protect sureties with special defenses), and

(4) policy or hostage-style secondary liability determinations. 249

When it comes to the code world, I have previously argued that the categories tend to lead to perverse results. Because of the power of code, it becomes possible to meter, monitor, and apportion revenues in such a way that almost any value-adding resource provider might be in serious jeopardy under several heads—it might be “contributory” or it might be “inducing” or it might trigger the special copyright style, or it might trigger some sort of hostage-style policy. Whatever it might be, the consequences are striking. One example will suffice: If I am a credit-card issuer or credit-card network and I have notice of some copyright infringement in cyberspace, then it is hard to resist the logic of the claim that I am secondarily liable. Because this is a coded world, it is probable that I am making some portion of my revenue as a direct result of the copyright-infringing acts, and I do have some power to control the offending conduct. The cases have thus far resisted this argument, but just barely. 250

It is crucial to the new focal point and invisible and attenuated trademark infringement cases that secondary liability be limited to reasonable technological accommodations and further controlled. I have already claimed as much in my prior article and I will have more to say about it in my forthcoming article.

249. See Folsom, Non-Neutral Principles, supra note 11.

250. See Perfect 10, Inc. v. Visa Int’l Service Assoc., 494 F.3d 788 (9th Cir. 2007) (imposing no secondary liability upon a payment system on notice that certain offending merchants were seeking payment from the payment system in respect of credit-card transactions by customers to whom the merchants had provided copyright-infringing materials, because the payment system’s involvement with the offending merchants did not amount to a sufficient financial interest and ability to control—over a spirited dissent by Judge Kozinski); Tiffany, Inc. v. eBay, Inc., 576 F. Supp. 2d 463 (S.D.N.Y. 2008), aff’d, 600 F.3d 93 (2nd Cir. 2010) (imposing no secondary liability upon the provider of an electronic marketplace despite the presence of trademark infringement by counterfeiters trading in the market, and despite substantial control over the marketplace, because of other factors including the provider’s substantial efforts to cooperate with the mark proprietor). See Folsom, Non-Neutral Principles, supra note 11, at nn.142–55 (discussing those cases).
IV. FINALE: INTEGRATING THE SOLUTIONS

The final portion of this argument is to show that the solutions are not only rule-specific and comprehensive, but that they are integrated. In this section, I will state each of the new rules, not for the purpose merely of repeating them one more time, but for the purpose of expressly integrating them with one another and with other mark-related regimes.

A. The Focal Point Offense

In an objective cyberspace that 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, invasive, 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.

B. Residual Cases of Likelihood of Confusion

The focal point offense already includes all cases employing invisible and attenuated trademarks as focal points, and so resolves all of them. Until the new offense is recognized, and for those residual cases in which the mark proprietor also cares to pursue trademark infringement, the “nature and place of use” analysis determines whether conduct constituting a focal point offense might also constitute likelihood of confusion. The fully specified “nature and place of use” factors for confusion take into account: (a) the nature of the conduct, the offending actor, and the supposed victim, pseudo-victims, and other persons affected; (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.

---

251. 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, nonrecoded focal points, including those that do not contain any trademark at all, violate the public interest in cyberspace itself, forfeit any claim to legitimate use, and already constitute misappropriation or theft, misrepresentation or fraud, or unfair competition.
C. The Common Remedy, Secondary Liability.

Given a focal point offense, or a likelihood of confusion caused by an invisible, expropriating, or attenuated use, the common remedy—a reasonable technological accommodation—includes one or more of a technologically reasonable and effective: (a) disclaimer, (b) notice, (c) redirect, (d) forced release, (e) reciprocal auction, and (f) opt-out/opt-in, plus (g) prophylactic measures and reasonable attorneys’ fees in appropriate cases. It takes into consideration whether there has been any polling or sampling, as well as the response to such queries. It should provide no more or less than the minimum necessary to fit the remedy to the offense and preserve the public interest in a robust and freely navigable cyberspace. It avoids the all-or-nothing approach of current trademark law in cyberspace and instead broadly permits, while modestly regulating, the use of focal points as an aid to access and navigation. It is the same remedy regardless which “cause of action” is pled.

Secondary liability is controlled and limited. It is controlled because it considers the nature of each party’s contribution, and the nature of that party as a predator or as a value-adding resource provider against specified criteria distinguishing one from the other. It is limited because it too requires no more than reasonable technological accommodations by the party that is subject to secondary liability.

D. The Relationship Between Focal Point Offenses and Trademark Infringement

I claim that there is a cyberspace focal point offense, apart from trademark law, and that it can be specified and should be recognized. When and if trademark infringement is asserted as a separate offense (or until the new focal point offense is widely recognized), then likelihood of confusion may be assessed according to a new “nature and place of use” analysis that specifies a new set of factors. The presumption is that the common remedy will ordinarily suffice under either theory as long as the trademark offense is invisible and attenuated.252 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 pattern obtains where there is an expression, like “shredded wheat” that has been determined to be generic, and hence incapable of legal protection as a trademark, but is nonetheless 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,
2012 / Poisoned Flowers, Part 1

Blinded Veterans patterns, then the common remedy, analogous to the simple precautions in such cases, should resolve the conflict. However, 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 trademark infringement adjudication under trademark’s new “nature and place of use” analysis and its new set of factors for assessing likelihood of confusion in cyberspace. This is especially true 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. For that indeterminate (but perhaps quite small) last category, 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 alleging fairly standard trademark infringement merely transposed to cyberspace.

market the product, and differentiate it in such a way as to avoid deception, misappropriation, or other acts of unfair competition. Id. at 118–22.

254. Blinded Veterans Assn. v. Blinded Am. Veterans Found., 872 F.2d 1035, 1043 (D.C. Cir. 1989). Similar pattern to the Shredded Wheat case, involving a senior user of “Blinded American Veterans” and a junior user of a similar expression, with similar results: even in the absence of trademark infringement, and though the junior party may continue to use, the junior is required to use with care to avoid unfair competition. Id. at 1041–43.

255. This would include those cases in which there is true preclusion-style initial interest confusion, and perhaps some others. See supra notes 210–213 and accompanying text (giving examples of true preclusion-style initial interest confusion).

256. 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 world wide 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, create relationships unlike any that can 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 that offered by the common remedy. I cannot 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 infra note 261 and accompanying text.
E. From Trademark-Related Law to Focal Points and Back Again

I propose the common remedy to unify the treatment of related and cognate mark-related offenses in cyberspace—including the UDRP,\(^{257}\) URS and other suggested proposals,\(^{258}\) ACPA,\(^{259}\) and dilution offenses\(^{260}\)—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. Most importantly, my goal is to design rules calculated to preserve the public interest in a robust and freely navigable cyberspace. This goal has led me to the focal point analysis that resolves the greater problem of which existing trademark and trademark-related law in cyberspace is merely a distracting subset. I propose that 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 then only in residual cases in which the proprietor might want to assert trademark infringement for additional trademark remedies beyond those provided by the common remedy, would we employ the new trademark-style “nature and place of use” analysis and new factor set to resolve the question of likelihood of confusion.\(^{261}\)

---


258. “URS” refers to the proposed Uniform Rapid Suspension System, offered in conjunction with the long-planned expansion of the global top-level domain names (gTLD’s). See, e.g., ICANN, IMPLEMENTATION RECOMMENDATION TEAM (IRT) REPORT 25–37 (2009), available at http://www.icann.org/en/topics/new-gtlds/irt-final-reportTrademark-protection-29may09-en.pdf (on file with the McGeorge Law Review) (one representative version of the URS proposal). There is some fluidity and other proposals have been floated for consideration; meanwhile the URS has gone through various iterations, was tabled indefinitely for a time, but now appears to be back in play. See Uniform Rapid Suspension System, Draft Procedure (Jan. 11, 2012), available at http://www.newgtlds.icann.org/en/applicants/agb/urs-1jan12-en.pdf (last visited Jan. 12, 2012) (on file with the McGeorge Law Review). One of the many advantages of my proposal is that it provides a rule-generating standard that is not dependent on the “flavor of the day” but is compatible with any number of plans, programs, and revisions to them promulgated by allied bodies: all of those are relevant in gauging the nature and place of use, and the “norms” that may be relevant factors to include when designing a coded solution, but none of them require retooling of my heuristic.


261. This makes room for the (currently reserved) category of remedies in addition to the limited common remedy, to which I refer in the last two sentences of note 256, supra.
The “nature and place of use” analysis is a generalized heuristic for addressing problems both in the code world generally and in cyberspace and in connection with focal points specifically. It is a principle that generates the “focal point offense” when it is specified to address the objective problem of dynamic focal points in a defined cyberspace. It also generates the new likelihood of confusion factors when it is specified to address the problem of invisible and attenuated use of marks in cyberspace. The same principle will also generate different, but equally productive, solutions for other problems in the code world involving different new technological uses that intersect with intellectual property (and other) law much more generally. This particular application of the “nature and place of use” to focal point and trademark-related offenses in cyberspace illustrates a way to design law “for” the code world by choosing an architecture supported by law, norms, and markets (prices). The forthcoming article will further illustrate the power of the new “nature and place of use” analysis.

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.

One feature of cyberspace is that it is defined and regulated by its architecture. Cyberspace is code, and code can be redesigned and rewritten. Freely written code can create focal point disputes in cyberspace because it enables dynamic addresses and magnets and because it permits operative roadblocks and detours. A purposefully regulated and redesigned code, then, can be made to resolve those disputes. A purposefully designed law can provide a legitimate fulcrum (and the “nature and place of use” analysis can provide a 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. But what if it did not? What if the offending actor had refused the simple accommodation of recoding, or what if the offended party had demanded more? 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 while upholding, not sacrificing, any foundational values of cyberspace.

My proposed solution actually makes good on Professor Lessig’s observation that we can deliberately choose optimal solutions in cyberspace. The focal point offense provides a specified and easily applied baseline (almost a “base

262. LESSIG, supra note 1, at 12–13.
263. See id. at 13 ("[W]hy not change the laws of nature to eliminate the conflict altogether?").
rule to dispose of most cases. The complementary “nature and place of use” analysis re-specified for trademark likelihood of confusion permits a rational determination of a new factor set to decide 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 remedy is deliberately designed to be limited and technologically effective. The limited remedy cures the harm, upon request and without destroying cyberspace or defacing the law itself. Controlled secondary liability prevents the accidental crippling of technology and also will minimize or reduce costly uncertainty about potential legal exposure that could hinder investment and commercialization of new technological uses.

V. WHAT REMAINS TO BE DONE—PRACTICAL IMPLEMENTATION

The new approach has three additional characteristics, making it well worth adoption by common law courts and practicing lawyers. It works. It is economically efficient. It is consistent with recognizable principles of existing law—it is authorized, principled, practical, and predictable. It is also urgently needed because the law appears to abhor a vacuum and there is a real danger that legislators, judges, or nongovernmental standard-setting bodies will, in response to real problems, implement (and continue to implement) bad regulation that

---

264. The parallels between “law language” and code might be worth exploring. See Folsom, Defining Cyberspace, supra note 8, at 78 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:

[i]f 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).

JavaScript Tutorial: Recursion, C-POINT.COM, http://www.c-point.com/javascript_tutorial/recursion.htm (last visited Apr. 6, 2010) (on file with the McGeorge Law Review). My proposed focal point offense may be considered something analogous to a base case for mark-type offenses in cyberspace, 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.
either deforms existing law, spoils the code world, or both. The goal of my next article is to persuade juridical 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.

A. The Proposed Solution: It Works

First, it works. It provides a highly practical resolution of cyberspace focal point conflicts because it gets to the correct result more reliably, for the right reason, and more-persuasively explained than any other proposed solution. The claim is that the new “nature and place of use” analysis (as a comprehensive solution unifying the focal point offense, the 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. In my forthcoming article, I will test the new analysis by giving illustrative examples; I will also test it against representative leading cases and against potential disasters waiting in ambush.

B. The Proposed Solution: It Is Efficient

Second, it is efficient. In my forthcoming article, I will allocate costs and benefits among cyberspace actors in a Pareto-optimal manner. Cyberspace actors 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 searchers, 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.\textsuperscript{267} For my present purposes, a “pirate” in cyberspace is anyone committing a focal point offense.\textsuperscript{268} The pirate deliberately alters the map, tampers with addresses or magnets, plants deceptive addresses or magnets, ambushes a user of focal points with uninvited, invasive, or false invitations, 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 or pseudo-victims whose interests have as of yet been rarely, if ever, considered in the existing case law.\textsuperscript{269}

\begin{footnotesize}
\begin{enumerate}
\item Pirates and plagiarists are defined terms in my work. See supra note 231. 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 ed., Columbia Univ. Press 2008) (1966) (seemingly conflating “plagiarism,” the norm against uncredited borrowing, with the legal offense of copyright infringement), with e.g., Folsom, Space Pirates, supra note 3, at n.226 (considering various senses in which the word is used, and specifying a meaningful usage), and Folsom, Non-Neutral Principles, supra note 11, at n.14 (specifying the term in order to make it meaningful).
\item In all senses in which I use the word, a “pirate” is someone who has committed a specified offense. More particularly, when the offense is “merely” against an extra-legal norm or against the law of nations outside the territorial jurisdiction of any one nation, it is often useful to call it, for example a “plagiarism” offense (when it involves unattributed, and frequently nonliteral, but norm-offensive copying of a copyrighted, patented, or public-domain product), or a “piracy” offense when there is no otherwise enforceable territorial law against it. But when the offense is against a territorial law by an actor within or otherwise subject to its jurisdiction, it is often more useful to name the law that has been broken (that is, the offense might be “trademark infringement” or “unfair competition” or “copyright infringement” or “patent infringement” or battery, murder, mayhem, or the like). This avoids the temptation to engage in a question-begging exercise or equivocal sleight-of-hand: calling someone a “pirate” does not necessarily mean the person has violated any existing territorial law. Calling “pirate” in relation to an act of “piracy” might express an essentially descriptive statement that some conduct is contrary to existing national or transnational law (or a prediction or forward-looking opinion that some fairly debatable conduct is likely to be ruled contrary to existing law); it could be a prescriptive recommendation that the law should be changed so that the conduct will become contrary to law; it may reflect a normative desire that the conduct should be contrary to law, or merely a claim that the conduct does in fact violate some specified norm. It helps to indicate which sense is indicated, and though I have used several of them, and often in a rule-specific prescriptive or normative sense, I hope the context makes it clear which sense I am using. Cf. generally Rebecca Tushnet, Copy This Essay: How Fair Use Doctrine Harms Free Speech and How Copying Serves It, 114 YALE L. J. 535, 537, 559 (2004) (noting the copyright debates over music and movie file sharing that have helped to make “copier” a synonym for “pirate”—and the perhaps unfortunate consequence of this, stemming in part from the common usage of “pirate” as a term that already signifies “copyright infringer”—often a question-begging verbal tautology when the question to be decided is whether the copying is or is not permissible). She argues for a more thoughtful analysis of “copying” prior to reaching any legal conclusion of infringement. Id.
\item Here I include 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, and who are far from confused.
\end{enumerate}
\end{footnotesize}
In addition to these actors, it is also important to consider the juridical actors who will need to decide cases, advise clients, and plan transactions, and those who are called upon to teach and to develop the law. Finally, it is important to consider the public interest, including the interest of users (curiously omitted from many of the decided cases) among whom are a number who desire to use focal points as markers to find branded goods, to comparison shop among competitors, or who are simply curious. There are also some who are deeply suspicious about the whole enterprise of creating some law “of” cyberspace and who deserve a reasoned answer, one that acknowledges there may well be any number of transactions that are enabled by the Internet and do not require any particular new law, but that there are at least some things in the code world that

270. Some are already proposing engaging methods for teaching “cyberlaw.” See, e.g., Ira S. Nathenson, Best Practices for the Law of the Horse: Teaching Cyberlaw and Illuminating Law Through Online Simulations, 28 SANTA CLARA COMPUTER & HIGH TECH, L.J. (forthcoming 2012), manuscript available at http://works.bepress.com/cgi/viewcontent.cgi?article=1009&context=ira_nathenson (Jan. 2012) (on file with the McGeorge Law Review). Others are attempting to organize the field into the more or less coherent form of a law-school casebook. E.g., PETER B. MAGGS, JOHN T. SOMA & JAMES A. SPROWL, INTERNET AND COMPUTER LAW CASES, COMMENTS, QUESTIONS (3d ed. 2010); PATRICIA L. BELLIA, PAUL SCHIFF BERMAN & DAVID G. POST, CYBERLAW PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE (3rd ed. 2006) (and sources cited, id. at pp. iii–v); RICHARD WARNER, GRAEME DINWOODIE, HAROLD KRENT & MARGARET STEWART, E-COMMERCE, THE INTERNET, AND THE LAW: CASES AND MATERIALS (2006); ROBERT P. MERGES, PETER S. MENELL & MARK LEMLEY, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE (4th rev. ed. 2007) (and sources cited, id. at pp. xxiii–xxiv); MARGARET JANE RADIN, JOHN A. ROTHCHILD, R. ANTHONY REESE & GREGORY M. SILVERMAN, INTERNET COMMERCE: THE EMERGING LEGAL FRAMEWORK (2nd ed. 2005) (and sources cited, id. at pp. vii–ix); RAYMOND S.R. KU & JACQUELINE D. LIPTON, CYBERSPACE LAW: CASES AND MATERIALS (2nd ed. 2006); RONALD J. MANN & JANE K. WINN, ELECTRONIC COMMERCE (2nd ed. 2004). I have selected these casebook editions, in part, because each is now over five years old. In addition to their other qualities, each of these would be improved by considering the foundational definition of a coded world and its distinctive places, and by examining the “nature and place of use” and challenging students and others to build an organic body of law suitable for a coded world in all of its manifestations and independent of the accidental technology of the day. See also MICHAEL L. RUSTAD, INTERNET LAW IN A NUTSHELL (2009) (explaining various technologies). The problems in the code world that are no longer around the corner, but here, coupled with the possibility of spectacular juridical error, see generally supra notes 89–98, require that we go beyond the cyber-hokum argument, see infra note 271, and start developing serious solutions to those coded problems that are unprecedented in ordinary space. Judge Easterbrook’s observation that we need to “develop a sound law of intellectual property, then apply it to [cyberspace],” Easterbrook, supra note 27, might be more useful were it turned on its head. Deliberately teaching (and designing) a law suitable for the code world and cyberspace might actually teach something about designing law more generally—perhaps a sound law of intellectual property might finally (and at long last) be created if we first developed a sound law for the code world and then applied it to intellectual property.

271. E.g., Easterbrook, supra note 27; Lee Gomes, Boomtown: Hot Field of Cyberlaw Is So Much Hokum, Some Skeptics Argue, WALL ST. J., July 1, 2002, at B1 (“Law involving the online world is hot right now. Law schools trying to stay current have courses in it . . . [but some skeptics] are deeply troubled by just about everything about this trend . . . [they argue that] something happening online shouldn’t be treated any differently by the law than if it occurred on Main Street.”); Joseph H. Sommer, Against Cyberlaw, 15 BERKELEY TECH. L.J. 1145, 1146 (2000) (“The steam engine . . . probably transformed American law, but the ‘law of the steam engine’ never existed.”); SCHECHTER & THOMAS, supra note 208, at 788 (dubbing at least some of the routine trademark controversies that occur in cyberspace as involving “shmyberspace”); Folsom, Defining Cyberspace, supra note 8, at 85–86 (quoting these and others to similar effect); id. at 95–101 (discussing some of the competing definitions, and nondefinitions, of cyberspace and citing sources before proposing a nonarbitrary, common sense definition suitable for legal decision-makers).
are distinctively different, and for which the ordinary law offers nothing but systemic failure and perverse results.

C. The Proposed Solution: It Is Authorized

Third, it is authorized, predictable, and principled. In my forthcoming article, I will demonstrate that the new offenses are recognizably derived from existing patterns of law already regulating misrepresentation, misappropriation, unfair competition (and, perhaps, restitution), and can easily coexist with trademark-related law. In short, I will support my claim that my proposal is authorized. 272

All this is to say that my proposal is ready for practical implementation. 273 It is also ready for further application elsewhere in cyberspace. 274 And it is ready for expansion into the code world beyond cyberspace. 275 The payoff is that my new proposal, once implemented, provides substantial dividends well beyond the problem of focal points and trademark law’s problem with invisible and attenuated uses. It is scalable, flexible, and adaptable.

VI. EPILOGUE

A. Designing Architecture (Law, Norms, Prices, and Code)

Granting that influencers of conduct in the code world include laws, norms, prices (and economics, more generally speaking), and architecture, 276 the question remains: “how, then, shall we choose” 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.

---

273. Against those who say that academic legal writing is “too abstract,” I claim that the technique proposed in this article is somewhat abstract but not “too much.” Because I use it to derive a standard that generates rules in specific form, it is completely practical and ready for implementation. See, e.g., Chief Justice Roberts on Obama, Justice Stevens, Law Reviews, More, Apr. 7, 2010, WSJ BLOG, http://blogs.wsj.com/law/2010/04/07/chief-justice-roberts-on-obama-justice-stevens-law-reviews-more/ (last visited on Sept. 27, 2011) (on file with the McGeorge Law Review) (reporting that “[Justice] Roberts said he doesn’t pay much attention to academic legal writing. Law review articles are ‘more abstract’ than practical and aren’t ‘particularly helpful for practitioners and judges.’”).
274. I claim that I have offered a resolution of the problem of focal points in cyberspace, ready for implementation. Further, I claim that the technique here proposed can be applied elsewhere in cyberspace. I claim the technique will also solve the problem of the library in space (sometimes known as the “Google Library” after its proponent, Google, Inc.) and that it might possibly solve the problem of patentable subject matter in cyberspace. In note 96 supra, I have stated some of the copyright and patent problems in cyberspace and suggested the solution.
275. I claim that the technique here proposed can be extended beyond cyberspace and into other places within the code world. In notes 90–98, supra, I have stated some of the problems in psberspace, ciphered space, the metaverse, virtual worlds, and the blogosphere. I believe the technique I am proposing is the key to resolving those problems in the extended code world.
276. LESSIG, supra note 1, at 86–90.

285
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, without necessary rivalry. However, 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 norm of the hitchhiker and of the hitchhiker’s guide). 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 do have a nature. These can, and do, create a virtue-defined norm for the code world that ought to be preferred.\footnote{By this I mean merely that a designed thing implies a function (or purpose), and that the function permits an evaluation based upon the degree of its performance or attainment; the evaluation is a conclusion that the thing is more or less excellent in comparison to its purpose; any virtue is an excellence relative to design. \textit{See} ARISTOTLE, NICOMACHEAN ETHICS, bk. I, at 63–64 (Hugh Tredennick ed., J. A. K. Thomson trans., Penguin Books rev. ed. 1976) (starting with an assumption that things designed for a purpose can be evaluated in light of their attainment of their purpose); Folsom, \textit{Defining Cyberspace}, supra note 8, at 93 (same). Had there been more space, I might have attempted to derive the same result as a deontological obligation to the extent that the design of cyberspace leads, by absolute necessity, to a generalizable set of rules based on pure reason. \textit{Cf.} IMMANUEL KANT, THE METAPHYSIC OF MORALS, Part I, at 9–11 (Mary Gregor ed. & trans., Cambridge Univ. Press 1996) (proceeding, analytically, from common knowledge to the determination of its ultimate principle). We could also have derived a more nearly rule-utilitarian or economic-based norm. But all of this would be redundant because my point is simpler. Designing a law for cyberspace is a choice; the choice is between competing norms, and this choice is not neutral. I have made it clear that, after defining both the common good of cyberspace and the harm of piracy in a specified manner, I believe the law both can and should choose against the pirate and in favor of the common good. I welcome a conversation on these issues, but the basic premise (that is, given the choice, the law ought to prefer good over bad results) seems inarguable because it is hard to think the opposite. I also thank Professor Alina Ng for pressing me to expand the moral-normative perspective beyond, or at least to make it clear that it could readily be extended beyond, the objectively derived values I had originally proposed (to move, as it were, from techno-Aristotelian to techno-Kantian analysis). We might also get to very nearly the same conclusion from principles based upon economic efficiency. \textit{Cf.}, e.g., LANDES & POSNER, \textit{supra} note 102 (analyzing intellectual property rules from an economic perspective that might possibly approach a normative maxim to avoid waste). There is room for, and I hope to encourage a more robust discussion of, alternative productive normative underpinnings to tech law.}

The economics of the code world, at least as it relates to dynamic focal points incorporating marks, must 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 an almost scarcity-free 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 their low acquisition cost. This drives out the opportunity for arbitrage otherwise existing in markets for dynamic focal
points, including those that incorporate marks. As a result, the market (or economic) incentive for focal point abuses is very nearly eliminated. Who would want to pay to reserve “lust.com,” “gluttony.com,” or “greed.com” when unbranded, common-source “lust” or “gluttony” focal points are available? And who would pay very much to reserve a branded (associative) focal point when all that does is to provide a directory assistance service (by the required notice and redirect) pointing any visitor to the brand proprietor, or to the other person(s) associated with the focal point? My proposed solution aligns the legal influencers with the economic and normative influencers, so that they 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, invasive, or false invitations, or (d) expropriates, blocks, or spoils focal points otherwise available. One particularly attractive aspect of the common remedy is that the same code that created the problems can be modified to alleviate those problems. 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. It is not merely neo-new tech or “neo-tech law,” comprising a techno-realism for the code world (although that is already a significant accomplishment). It is part of the search for a common morality suitable for a rule of law in a global and tech age. The law and morality movement (or the move to a normative jurisprudence in accordance with specified principles, or a specified “restatement of the obvious”) 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 this global–tech era.

I trust the reader will not conclude that my own focus on the laws of the United States is due to anything other than the fact that I must start somewhere, and this is where I am. The problem of trying to design sensible regulations for the code world is certainly not limited to the United States but is global. Because of the interconnectedness of the code world, however, bad law in the United States can lead to bad law globally. At the same time, there is reason to hope that better law in the United States might be a benign influence globally. Though I do argue for a cyberspace that is as “open” as is reasonably possible (open, that is, to

278. This is an example of “free-riding on the free-rider.” In Appendix A, infra at 295, I discuss this concept in connection with the case of Superman and Mr. Mxyzptlk.

279. See, e.g., The Catholic Univ. of Am.’s Ctr. for Law, Philosophy and Culture Symposium: A Common Morality for the Global Age (Mar. 27–30, 2008), available at http://clpc.cua.edu/internationalsymposium (on file with the McGeorge Law Review) (an international symposium convened to “provide[] a forum for inquiry into the meaning of law and legal institutions for culture and the human good”).
access, navigation, and information activity, by augmented presences, in a background of reasonable trust), there is nothing else in my proposal that is limited to the United States. In fact, some other nation might be the first to adopt my proposals. The specific tailoring of my proposals for any other nation in light of its own particular existing law is a problem I cannot address in this paper, but which I invite others to resolve. I believe the principles are applicable and that the same “nature and place of use” heuristic can generate similar rule-specific determinations. At the very least, my proposal will provide a vocabulary that will clarify the issues, so that if there should be disagreement, the terms of any debate may be more clearly understood.

In proposing an architecture designed to be congruent with deliberately selected norms, I am not alone. This article claims the new “nature and place of use” analysis, the focal point offense, and the new factors for the residual cases of trademark infringement fit comfortably within the capability of juridical agents, and are recognizable transformations of existing law capable of principled, practical, and predictable application. Most significantly, this approach finally answers the question—how to choose the architecture of the code world?—by 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 that distinguish one from the other. In another sense, the end is merely to provide a clearly marked common good, as an object or target, so that we might know where we are trying to go, and so that juridical agents might figure out whether they are more nearly taking us there or somewhere else.

280. See generally, e.g., ROBERT P. MERGES, JUSTIFYING INTELLECTUAL PROPERTY (2011) (deriving a normative concept from a Lockean and Kantian synthesis, and qualifying it as fair in accordance with the dictates of Rawls; all of it leading to mid-level principles—proportionality, efficiency, preservation of a public domain, and dignity—that are consistent with economic or utilitarian notions and that together create a common normative framework that permits a policy debate without requiring any agreement on ultimate foundational issues, and leading to a practical payoff in resolving leading-edge legal challenges); ALINA NG, COPYRIGHT LAW AND THE PROGRESS OF SCIENCE AND THE USEFUL ARTS (Elgar Law, Tech. and Soc’y Series) (2011) (framing the copyright system within a normative legal order, and claiming that sustainable progress in copyrighted works of authorship is best achieved through application of basic principles of ethics and morality); David W. Onderbeck, A Virtue Ethics Approach to the Biotechnology Commons (or, The Virtuous Penguin), 59 MAINE L. REV. 316 (2007) (proposing a virtue ethics approach to biotechnology law). And see supra note 277 (indicating how my prior work, especially Defining Cyberspace, supra note 8 and Space Pirates, supra note 3, could easily be grounded not only upon Aristotelian virtue ethics in cyberspace, but also on Kant’s imperative, and tested by economic efficiency). These are all examples of integrated law, norms, markets, and architecture as telegraphed by Professor Lessig, supra note 1.

281. See generally Folsom, Evaluating Supernatural Law, supra note 114.
B. Closing Postscript: Where’s the Dog? (Economics in the Code World)

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.\(^{282}\) 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.”\(^{283}\) But the pricing reflects the underlying valuation of goods in a world of scarcity and uniqueness, not a coded world. Accordingly, we might well 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.”\(^{284}\)

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 “efficient outcome” in ordinary space.\(^{285}\) 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.”\(^{286}\)

The contrast between the economics of the coded space and ordinary space is stark. The expedient of rewriting the code, at least in some places within the code world, very nearly 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, $1,000, or millions of dollars; nor need he ask whether Dank valued his dog at $600, $800, or millions of dollars. In cyberspace, all we need to know is that at least some of the code may be reasonably rewritten at zero or negligible cost. When that can be done the law ought to require it. For


\(^{283}\) Id. at 211.

\(^{284}\) Id.

\(^{285}\) Id.

\(^{286}\) 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? Cf. SILVERADO (Columbia Pictures 1985) (asking “where’s the dog?”), available at http://www.youtube.com/watch?v=sIJUBys2Fbs (last visited Dec. 20, 2011) (on file with the McGeorge Law Review) (excerpting segments of the motion picture asking about the whereabouts of the dog).
the equivalent of a nickel or a dime, and for a higher price voluntarily paid when it adds real value, the parties can actually dispose of what would otherwise be an expensive or frustrating legal dispute. 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 an added premium to do without.

It is striking, after all the years spent pretending to “Coasian conditions” of near-zero transaction costs, to actually find, hiding in plain sight, at least some places within a coded world where those hypothetical conditions really exist. 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.”287 And contrary to the correlative notion that the starting point does not matter, the starting point, and the law’s incentives, do make a difference in the code world by setting the equilibrium points. 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.288

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. Concepts no more difficult than high school-level notions of algorithmic thinking, abstraction, and elegance are in play.289 Techniques as straightforward as sequential
processing, conditional execution, iteration, decomposition, and computing a result by calling a function are on display. And when code-based problem-solving patterns as clear as establishing a requirements specification, designing a solution, implementing the solution in code, and testing the code (and repeating until satisfied) are the common property of school children, it is unseemly for the “law” to be so truant in its slow advance into the code world. It is time to stop feigning an antic disposition and simply to design a law for cyberspace and the code world. Like Hamlet eventually realized, it is time to decide and then to act.

VII. CONCLUSION

In this article, I demonstrated that a focal point offense in cyberspace can be specified, and that any residual likelihood of confusion inquiry can be resolved by a new set of likelihood of confusion factors. The new “nature and place of use” analysis generates both of these particular rule-specific techniques. I claim the focal point offense and the new factors provide a rule of thumb that would dispose of cases efficiently, and would get to the correct result for the right reason, persuasively explained. My prior articles argued that 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, without creating new problems of doctrinal creep, reverse doctrinal creep, and special pleading for special factions in cyberspace.

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
2012 / Poisoned Flowers, Part 1

fact, it is the current null set of equivocations, innovations, recently invented or surprisingly rediscovered 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, what is truly daunting in its complexity is the current approach, which requires juridical actors to attain or pretend to a level of expertise in computer and network theory and to take seriously various passing fancies in technological implementations, not to mention trends in badly composed metaphor divorced from the objective reality of a coded world. 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 to continue to pursue them.

But quite the opposite is true. Mastery of the new terminology of the “nature and place of use” analysis, the specified focal point offense, and the new likelihood of confusion factors proposed in this article is a rather straightforward exercise. Some of the new offending uses in cyberspace are “attenuated” in the sense they do not make an immediate association, much less an affixation of a designation to goods or services. But they are certainly “uses” of a designation made by an actor in marketing a product. Some of the offending 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; 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. Still other 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, detour, and/or mark in cyberspace. To be sure, these are not the ordinary uses 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 and that are rationally assessable by reasonably obtainable evidence. They give a name to the already-existing phenomena, thereby permitting and facilitating a designed solution.

The invisible, attenuated, and expropriating uses of focal points containing trademarks—markers or spoilers functioning as an address, magnet, and/or mark, or as a roadblock or detour—are the paradigmatic problems of trademark-related law in an objective cyberspace. This article has demonstrated that the independently actionable focal point offense and the fully specified new likelihood of confusion factors generated by considering 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 correct result for the right reason, persuasively explained. Their costs and benefits make sense because the focal point offense and the new factor allocate
them fairly among the primary and secondary 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 factors for residual trademark infringement cases ought to be embraced as the solution to invisible, attenuated, or expropriating uses in cyberspace. In a subsequent article (in a forthcoming issue of this volume of the *McGeorge Law Review*), I will demonstrate that the focal point offense and the new factors have three additional 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. The existing law has nothing to lose but its incoherence.
2012 / Poisoned Flowers, Part 1

* * *

294
McGeorge Law Review / Vol. 43

APPENDIX A: SUPERMAN AND MR. MXYZTPLK

Superman cover art, 295
Introducing “The Mysterious Mr. Mxyztplk!”
From SUPERMAN Vol. 1, No. 30 (1944), © 1944, DC Comics.

I use the Superman–Mxyztplk\textsuperscript{296} example as a running, and unifying theme throughout this article.\textsuperscript{297} It concretely demonstrates how the general idea of resolving the poisoned-flowers and the dead dog (the other running example used in this article)\textsuperscript{298} by rewriting code is a key to designing a specific solution that can satisfy everyone, which is to say that the solution is game suboptimal or Pareto-superior. The problem is that the general idea of rewriting code, by itself, cannot do anything until it is translated into rule-specific form. I use a powerful rubric, the “nature and place of use,” to transform, translate, and connect the poisoned flowers idea to one or more concrete proposals, each specified as appropriate for the particular place in the code world, and for the particular offending use that is occurring there. This article specifies the nature and place of use for recoding and resolving focal point and trademark-related conflicts in cyberspace. Given the ubiquity of “Mxyztplk” in this article, I thought it well to include this appendix to make the literal reference more clear, and more explicitly to explain how it makes concrete the proposal that I have presented in this article.

A principal claim of this article is that a law deliberately designed for cyberspace can influence norms, prices, and architecture in the code world. The specified rules that I propose will, among other things, require an effective notice or redirect from one vanity address to another location. This has the effect of eliminating the opportunity for arbitrage inherent in current practice.\textsuperscript{299} Under current law, an actor might expropriate a valuable focal point, for example, “superman.com,” by forming an easily remembered vanity web address highly “guessable” by surfers seeking to find information about, say, “Superman.” Under current law, the mark proprietor, another person having a legitimate interest in the expression, or a community of interest in things signified by the expression, might either be forced to spend excess litigation fees (beyond the cost of simple UDRP or beyond the cost of simple summary judgment without the need for extensive discovery) to possess the address, or might instead simply offer to pay the expropriating actor a price well in excess of the actor’s cost to

\textsuperscript{296} For the variant spellings (flipping the “p” and the “t” in “Mxyztplk”) see infra text accompanying note 303.

\textsuperscript{297} The Superman example recurs throughout this article. See supra pp. 199, 212–15, and 237 for some of the Superman–Mxyztplk discussion.

\textsuperscript{298} The poisoned flowers and the dead dog example, borrowed from Professor Lessig, recurs throughout this article. See supra pp. 1, 9–14, 21 (nn.54–55), 32 (n.88), 37–38, 72 and 76 for some of the poisoned flowers/dogs discussion.

\textsuperscript{299} I propose a modestly transformed law, designed and specified deliberately to select an architecture of minimal control to preserve the values of cyberspace. It changes the price, therefore changes the economics, and as a result, supports the norms of open access, free and unhindered navigation, and robust information-activity by increasing the trust necessary to protect the augmented presence of surfers in cyberspace who use focal points as part of the virtual map. I believe this must be the sort of thing Professor Lessig had in mind when prescribing choice of code to reconcile laws, norms, markets, and architecture in cyberspace. See LESSIG, supra note 1.
obtain the address without litigation. Regardless of the method, under current law the new owner would then be the sole possessor of the focal point address, which raises yet additional problems in respect of other legitimate users of the focal point.

Part of my proposal is a “common remedy” that would require reasonable technological accommodations, including effective notice or a redirect. As a result, the actor who possesses any focal point address is required to provide an effective means redirecting traffic (visitors) to the location of the mark proprietor(s) (or other persons, places, or communities of interest associated with the focal point), the choice being left to the visitor.

Therefore, a mark proprietor could establish a site at an address which is difficult to remember or to spell (like “mxyztplk.com”) but which will work perfectly well to serve those who were looking for the mark proprietor and who first hit the easily guessable vanity address (“superman.com”). This is because even though navigating to “superman.com” would take the visitor to a site not sponsored by the mark proprietor, it would at the same time provide the visitor with an effective choice by the technologically effective expedient of the notice or redirect. By a simple click on the redirect list, the visitor’s augmented presence would be redirected to a site that is sponsored by the mark proprietor. This removes any likelihood of confusion, and it adjusts the interests of each of the parties, preserving the legitimate concerns of each.

This solution permits (1) the visitor to decide what she wants to see and where she wants to go. It protects (2) the mark proprietor; indeed, it allows the mark proprietor to “free-ride” on the free-rider, as a matter not only of poetic justice, but of actual justice. It also protects (3) those independent actors who are making a legitimate noninfringing use of another’s mark—that is, an actor who is using another’s trademark in cyberspace, not to appropriate the good will of the mark proprietor, but to provide value-adding information using the mark as a focal point to attract traffic by what is analogous in cyberspace to a type of nominative or descriptive fair use in ordinary space (what it actually is—a low search cost, user-oriented comparison shopping/finding tool under the control of the user, and which can actually take a user’s augmented presence to a location—is unique to cyberspace and without any direct parallel in ordinary space). An independent actor who is actually providing some service will, by hypothesis, be able to hold the attention of a visitor even after giving an effective opportunity for the visitor to click through to one or more mark proprietor(s) or other persons, places or communities of interest associated with the focal point; but those actors who don’t provide any service or information will not hold their visitors.

300. This appendix is itself a fine illustration of the point. The site that provided the key which eventually led to the art work I was seeking, and which appears in this appendix includes “Superman” as an embedded term. Because the site provider is serving a need, some visitors would remain on that site, even if there were a required redirect to “DC Comics.” My proposal would permit the continued use of “Superman Supersite.com” but with, at most, a redirect. If the site were empty, a sham, or some sort of false invitation, then
2012 / Poisoned Flowers, Part I

Moreover, the reasonable technological accommodation of my solution also shelters and provides a safe harbor to resource providers (who might otherwise face potentially ruinous secondary liability), and it even allows scalliwags and pirates to continue their uses (the redirect having rendered them essentially harmless). Finally, it protects (4) the public interest in a full and free, robustly navigable cyberspace, trustworthy enough so that otherwise vulnerable augmented presences can engage in the information-activity for which cyberspace serves the common good.

My approach is first to define space pirates and predators in a meaningful way, using the “nature and place of use” as a guide, and then to design a law more nearly apt to reform pirates into useful citizens than to stop the signal that permits access, navigation, and information activity in cyberspace (as would be the case if there were to be overly blunt secondary liability imposed upon value-added resource providers). As observed by Zoe and Wash, two crew members of the noted space pirate, Captain Malcolm Reynolds, there ought to be some consequences to their actions, perhaps jail. But my proposal is aimed at regulating the code world, not stopping the signal. Because of the limited remedy and the power of countervailing code to remediate offending code, the consequences will be just enough to make cyberspace work; with technological accommodations, we don’t need to send unconventional users of focal points to jail, nor need we impose such draconian penalties upon value added resource providers as would distort the good of cyberspace. As long as there are reasonable technological accommodations, the law can help to make cyberspace work for the common good.

By the way (and the interested reader may find yet more information than this introductory set of facts about Superman and this fellow, Mxyztplk, than contained in the few highlights appearing below), here is some information about the character:

---

most if not all of those who were attracted to it would click away from it almost immediately. The new common remedy sorts out “fair” use from foul, and distinguishes value-adding resource providers from predators, simply by aligning laws, norms, prices, and architecture. It naturally distinguishes the hitchhikers’ guide and value-adding resource providers from pirates, predators, and spoilers. By the way, it does not prevent even pirates from continuing in their occupation, it just drives out the profit, and hence it probably drives most pirates into a more honest form of employment, thereby pressing them into service; serving the common good of access and information in cyberspace. See W. S. GILBERT & ARTHUR SULLIVAN, THE PIRATES OF PENZANCE, act 2, no. 24, at 144 (Ephraim Hammett Jones & Carl Simpson eds., Serenissima Music 2001) (1879) (“When a felon’s not engaged in his employment / Or maturing his felonious little plans / His capacity for innocent enjoyment/ Is just as great as any honest man’s”).

301. Cf. SERENITY (Universal Pictures & Barry Mendel Productions 2005) (“You can’t stop the signal . . . . Everything goes somewhere and I go everywhere.” (spoken to Captain Malcolm Reynolds, shortly before an alliance of federated planets tried to do just that)).

302. Firefly: Serenity (Pilot episode) (Fox television broadcast Dec. 20, 2002). Zoe: “I know something ain’t right.” Wash: “Sweetie, we’re crooks. If everything were right, we’d be in jail.” Id.
Mister Mxyzptlk (roughly pronounced Mix-yez-pit-lick, also nicknamed Mxy) [note: in this popular rendering, and popular pronunciation, the “p” precedes the “t”] is a fictional super villain who appears in DC Comics’ Superman comic books. He was created by Jerry Siegel and first appeared in Superman (volume 1) #30 (September 1944).

“Mr. Mxyztplk” (as his name was originally spelled) [note: in this original rendering, the “t” precedes the “p” and this is the form I use throughout my article] was introduced as an imp from the fifth dimension. Not being bound by our physical laws, he could do things that seemed to be magical. In his first appearance, Mxyztplk wreaked havoc across Metropolis by using his powers to pull all manner of pranks. He soon told Superman that he was a jester in his home dimension, explaining why he used his powers to play practical jokes. Superman soon discovered he was able to send Mxyztplk back to the fifth dimension by making him say his name backwards.

Originally, Mxyztplk had designs on conquering the planet for himself, but soon settled for tormenting Superman whenever he got the opportunity. His only weaknesses were that he could not stand being ridiculed and if he said or spelled his name backwards, [Klptzyxim (pronounced kil-pit-zee-zim)], he was involuntarily sent back to his home dimension for a minimum of 90 days. Mxyztplk would often look for ways to counter the latter weakness, but he always proved gullible enough for Superman to trick him time and time again.

Mxyztplk appeared originally as a small bald man in a purple suit, green bow tie and purple derby hat. This was changed to a futuristic looking orange outfit with purple trim in the mid-1950s, although the hat remained. At around this time the spelling of [Mxyztplk’s] name changed (by mistake) to “Mxyzptlk.”

You will notice that the already-odd name is further complicated by the flipping of the “p” and the “t” for no apparent reason. The beauty of the redirect, as described in my proposed resolution of the focal point problem, is that all of this is invisible to the surfer, and is a matter of indifference to the mark proprietor (who will not need, as some statements of current law seem to require, to warehouse or register all conceivable variant or “trapping” addresses). A click on the “superman.com” site will lead to a link to DC Comics, and that is all the user needs to know. The mechanism, invisible to the user, but apparent to a virtual machine in cyberspace, will do the rest, regardless whether it is sending the user

303. SUPERMAN SUPERSITE, see photo credit, supra note 295, at Appendix A. I have not independently verified the entry, and I leave it to Superman scholars to investigate this further, and to find and confirm the original sources in hard copy.
2012 / Poisoned Flowers, Part 1

to “mxyzptlk.com” or “mxyztplk.com” (or some other address)—that’s part of the beauty of code, and it very well illustrates the neo-tech law approach of which my article is perhaps the first example.304