LAW, GEOGRAPHY AND CYBERSPACE: THE CASE OF ON-LINE TERRITORIAL PRIVACY

DANIEL BENOLIEL*

TABLE OF CONTENTS

* Internet Society Project (ISP) Visiting Fellow, Yale Law School and J.S.D. candidate University of California, at Berkeley, School of Law (Boalt Hall). This study was funded by the Informational Technology Research (ITR) research grant, University of California at Berkeley, The Center for Information Technology Research in the Interest of Society (CITRIS). This study also won the prize for best student article competition in the Fourteenth Annual Computers, Freedom & Privacy Conference. For their most helpful comments and support, I am indebted to Pamela Samuelson, Mark Lemley, David Post, Dan Hunter, Julie Cohen, Edward Soja, Orin Kerr, the Chief Scientist of CITRIS - James Demmel and David Wagner. Any inaccuracies are my responsibility. For further questions or comments, please email me at: Daniel_b@berkeley.edu.

ABSTRACT

Territorial privacy, one of the central categories of privacy protection, involves setting limit boundaries on intrusion into an explicit space or locale. Initially, the *Restatement (Second) of Torts*, which defined the privacy tort of intrusion as applied by courts, most notably designated two classes of excluded areas: "private" places in which the individual can expect to be free from intrusion, and "non-private" places, in which the individual does not have a recognized expectation of privacy. In the physical world, courts ultimately held, almost uniformly, that the tort of intrusion could not occur in a public place or in a place that may be viewed from a public place.

Cyberspace, on the other hand, which lacks a public sphere, does not have a balanced territorial privacy policy. Instead, based on the category of database privacy protection, only a private privacy legal rule was adopted—and too widely so. One of the main explanations for this anomaly, in fact, derives from cyberspace's unique architecture. While the physical world is subject to a default rule of a continuous public sphere, which is then subject to distinct proprietary private sphere allotments, cyberspace architecture, on the other hand, imbeds a different structure. In the latter, apart from the Internet's "public roads" or backbone transit infrastructure, which is distinctly regulated according to telecommunications and antitrust law, the present default rule contains a mosaic of private allotments—namely, neighboring proprietary websites.

This anomaly is even more acute given that the U.S. government, the Federal Trade Commission ("FTC") and theoreticians alike have, thus far, developed neither comprehensive nor supportive boundary theory that could maintain territorial privacy. All three, instead, have implicitly or explicitly only considered

technocentristic boundary approaches. From a legal perspective the factual truths or scientific hypothesis underlying the existence of on-line spatiality, as discussed notably in the works of Johnson and Post, Lessig, Hunter, Lemley, and others, should, instead, be only a parameter in establishing legal truth. In compliance with what is an alternative localist boundary approach, this study suggests that law could construct a legal fiction of on-line locales through which territorial privacy, ultimately, could be integrated into cyberspace privacy policy at large. In the future, other territorially based laws, such as those within taxation, property, copyright, or the torts of trespass, could follow.

INTRODUCTION

A. *Information Privacy: The Imperfect Vision for Computer-related Privacy*

Privacy is a challenging legal concept and is difficult to define.[1] No bright-line rule indicates whether an expectation of privacy is constitutionally reasonable.[2] The concept of privacy does not have a single interest, but rather several different dimensions or categories that are not just observed, but are also legally constructed. The concept of privacy is generally divided into four categories.[3] The first category is bodily privacy, which addresses issues related to the physical integrity of the individual against invasive procedures through the tort of trespass to the person. Originally, the law provided a remedy solely for physical interference with the life and property of the individual.[4] The second category concerns the privacy of communications, which relates to the First Amendment's freedom of speech and association, where an individual is granted the right to communicate freely among peers.[5] It covers the various interests of individuals in communicating among them-

---

[1] *See, e.g.*, Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 422 (1980); JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 3 (1992); Hyman Gross, *The Concept of Privacy*, 42 N.Y.U. L. REV. 34 (1967); Raymond T. Nimmer, *Privacy Rght vs. Public Right*, INFORMATION LAW, November 2001, ¶ 8:31.

[2] *See* O'Connor v. Ortega, 480 U.S. 709, 715 (1987).

[3] *See, e.g.*, Gavison, *supra* note 1, at 433; Joseph I. Rosenbaum, *Privacy on the Internet: Whose Information is it Anyway?*, 38 JURIMETRICS J. 565, 566-67 (1998).

[4] As early as 1891, the Supreme Court declared: "No right is held more sacred, or is more carefully guarded by the common law, than the right of every individual to the possession and control of his own person . . . ." Union Pac. Ry. Co. v. Botsford, 141 U.S. 250, 251 (1891). *See* MORRIS L. ERNST & ALAN U. SCHWARTZ, PRIVACY: THE RIGHT TO BE LET ALONE 47 (1962); Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 266 n.119 (1977).

[5] *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514, 526 (2001); United States v. McRae, 156 F.3d 708, 711 (6th Cir. 1998); Kee v. City of Rowlett, 247 F.3d 206, 216-17 (5th Cir. 2001).

selves using various forms of communications. The third category is information privacy, which concerns the control and handling of personal data.[6] The constitutional right to information privacy is a derivative of the Supreme Court's substantive due process "right to privacy" cases, such as *Griswold v. Connecticut*[7] and *Roe v. Wade*.[8] The fourth category, and the focal point of this study, is territorial privacy, which involves setting limit boundaries on the intrusion into an explicit space or locale.[9] It is important to focus on not only the disruptions, but also the practices that have been disrupted. We often refer to aspects of these practices as "private matters." "In other words, we say that certain things, places, and affairs are 'private.'"[10] Initially, courts designated two classes of excluded areas: (1) "private" areas, such as a home,[11] or a reserved hotel room,[12] in which the individual can expect to be free from intrusion;[13] and (2) "non-private" areas, in which the individual does not have a recognized expectation of privacy.[14] The designation of an area as "private" protected the personal information located within from intrusion and governmental seizure. The *Restatement (Second) of Torts* incorporated these views into the comments to section 652B,[15] which defines the privacy tort of intrusion.[16] Thus,

---

6 *See* Gavison, *supra* note 1, at 433. Posner defines it as an individual's "right to conceal discreditable facts about himself." RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 46 (5th ed. 1998); RICHARD A. POSNER, The ECONOMICS OF JUSTICE 272-73 (1981).

7 381 U.S. 479 (1965).

8 410 U.S. 113 (1973). In this landmark privacy case, the Court upheld that the right of privacy includes the right to make one's own decisions about activities related to marriage, procreation, contraception, abortion, family relationships, and education, or a subsidiary category of privacy, known as "decisional privacy." *Id. See* Whalen v. Roe, 429 U.S. 589, 599-600 (1977) (by using a spatial metaphor, the Court reaffirmed that the constitutionally protected "zone of privacy" jointly protected the "individual interest in avoiding disclosure of personal matters," with the individual's "independence in making certain kinds of important decisions.").

9 In boundary theory, the terms "space," "locale," "sphere" or "area" have separate spatial meanings that will be distinguished later in this article. *See* discussion *infra* Part II.

10 *See, e.g.*, William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389-91 (1960); Daniel J. Solove, *Conceptualizing Privacy*, CAL. L. REV. 1087, 1131 (2002); *see also* JOHN STUART MILL, ON LIBERTY 11-13, 75-77 (Norton ed. 1975) (emphasizing public and private locales).

11 *See* Clinton v. Commonwealth, 130 S.E.2d 437 (Va. 1963), *rev'd sub nom.* Clinton v. Virginia, 377 U.S. 158 (1964).

12 *See* Stoner v. California, 376 U.S. 483 (1964).

13 *See* Harkey v. Abate, 346 N.W.2d 74 (Mich. Ct. App. 1983).

14 *Id.*

15 For an exception recognizing a cause of action of privacy intrusion in the public sphere, see RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977). *See also* Daily Times Democrat v. Graham, 162 So. 2d 474 (Ala. 1964); Andrew Jay McClurg, *Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places*, 73 N.C. L. REV. 989, 1045-55 (1995) (upholding "public privacy" paradigm and a tortious cause of action).

16 *See, e.g.*, RESTATEMENT (SECOND) of TORTS, § 652B cmt. c. The RESTATEMENT (SECOND) OF TORTS § 652B defines a tort as the intrusion into the seclusion of an individual. It is intended to protect against intrusions, physical or otherwise, "upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly

courts have almost uniformly held that the tort of intrusion cannot occur in a public place or in a place that may be viewed from a public place.[17] Therefore, on a public street, or in any other public place, the plaintiff has no legal right to be alone.[18] The circumstances themselves in such cases do not involve seclusion,[19] and it is not an invasion of privacy to do no more than follow the plaintiff about and watch the plaintiff there.[20]

The territorial facet of privacy has not been adequately applied to privacy in cyberspace because cyberspace is not a physical space, and any analogy to a physical space is a poor one.[21] Instead, only a vision of information or database privacy has been proffered. This involves the three basic ways in which personal information can be digitally transmitted and collected from computers and over the Internet—through websites, personal computers, and network service providers such as Internet service providers ("ISPs").

The first issue, the focal point of this study, is privacy policies for website collection of personal data.[22] Websites collect personal data through cookies, registration forms, and sweepstakes that re-

---

offensive to a reasonable person." *Id.* The federal government and courts in at least twenty-eight states have explicitly or implicitly recognized this privacy tort and adhere to the definitions offered in the RESTATEMENT (SECOND) OF TORTS §§ 652B-652E (1977). *See* W. PAGE KEETON ET AL., PROSSER & KEETON ON THE LAW OF TORTS 851 (5th ed. 1984); RESTATEMENT (SECOND) OF TORTS, *supra*, at Reporter's Notes (a list of practically all of the states and the federal government which uphold the RESTATEMENT (SECOND) OF TORTS § 652B Tort of Invasion).

17 *See* KEETON, *supra* note 16, at 855-56; Prosser, *supra* note 10, at 391-92; McClurg, *supra* note 15, at 1025; Phillip E. Hassman, Annotation, *Taking Unauthorized Photographs as Invasion of Privacy*, 86 A.L.R.3d 374; *see also* Hartman v. Meredith Corp., 638 F. Supp. 1015, 1018 (D. Kan. 1986); Fogel v. Forbes, Inc., 500 F. Supp. 1081, 1087 (E.D. Pa. 1980); Pemberton v. Bethlehem Steel Corp., 502 A.2d 1101, 1116-17 (Md. Ct. Spec. App. 1986); Forster v. Manchester, 189 A.2d 147, 150 (Pa. 1963); Foster v. Livingwell Midwest, Inc., 865 F.2d 257 (6th Cir. 1988); Int'l Union v. Garner, 601 F. Supp. 187, 191 (M.D. Tenn. 1985) (mem.).

18 *See* KEETON, *supra* note 16, at 855 n.68; Hassman, *supra* note 17.

19 *See, e.g.*, Granger v. Klein, 197 F. Supp. 2d 851 (E.D. Mich. 2002) (under Michigan law, publication in high school yearbook of photograph showing student urinating with his genitalia visible did not constitute intrusion into seclusion by school's principal, assistant principal, yearbook advisor, and yearbook publisher, since they did not obtain photograph by objectionable means; photograph was snuck into photo collage by student's friend, and yearbook was edited by other students).

20 *See* KEETON, *supra* note 16, at 855 n.68; Hassman, *supra* note 17.

21 *See* discussion *infra* Part II.A.1-2.

22 For surveys supporting the widespread practice of data collection by websites, see, for example, Electronic Privacy Information Center, *Surfer Beware: Personal Privacy and the Internet, at* http://www.epic.org/reports/surfer-beware.html (last visited April 4, 2005) (suggesting that nearly half of the 100 most popular websites collected information from users); FED TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS (July 1999) (referring to Georgetown Internet Privacy Policy Survey, *at* http://www.msb.edu/faculty/culnan/gippshome.html and suggesting that up to eighty-five percent of websites collect personal information from consumers), *available at* http://www2.cddc.vt.edu/www.eff.org/pub/Privacy/199907_ftc_online_privacy_report.html (last visited Apr. 15, 2005).

quire surrendering e-mail addresses and other information.[23] Other invasions of privacy relating to websites involve archives of comments made on the "Usenet"[24] or to "listservs,"[25] and the deceptive promises that websites sometimes make about privacy practices.[26] Originally, the computer information privacy policy followed the U.S. Department of Health and Education's information privacy policy, promulgated in 1973.[27] The United States federal on-line information privacy policy was also directly influenced by the strict information privacy protection policy that was adopted internationally by the Organization for Economic Cooperation and Development ("OECD") in 1980.[28] These guidelines were based on eight principles of information privacy: (1) collection limitation; (2) data quality; (3) purpose specification; (4) use limitation; (5) transparency of information collection practices; (6) security of stored data; (7) individual participation; and (8) accountability.[29] In implementing these principles, the Federal Trade Commission ("FTC") ultimately imported these guidelines' information privacy orientation.[30] It did so in outlining a set of Fair Information Practices ("FIPs") which regulate the collection and use of consumer-

---

23 MICH LAW REVISION COMM'N, PRIVACY AND THE INTERNET: A STUDY REPORT TO THE MICHIGAN LAW REVISION COMMISSION, MICHIGAN LAW REVISION COMMISSION THIRTY-FIFTH ANNUAL REPORT 22 (2000), *available at* http://www.milegislativecouncil.org/mlrc/2000/PrivacyandInternet.htm (last visited Apr. 9, 2005).

24 Usenet allows participants to post communications into a database that others can access. *See id.*

25 Listservs are listings of names and e-mail addresses that are grouped under a single name. *Id.*

26 *Id.* Some web surfing instructions may not be translated into sensory effects at all, but instead, direct the browser to take certain actions, such as changing the size of the window, opening a new window, or reloading the page after a given amount of time. *See* Rajesh Vijayakumar & Devi S Nadh, *A Beginner's Guide to JavaScript, at* http://www.javascriptguide.com (last visited April 14, 2005); Netscape Assistance, *An Exploration of Dynamic Documents, at* http://wp.netscape.com/assist/net_sites/pushpull.html (last visited Apr. 11, 2005). In addition, web surfing takes other technical forms, such as retrieving stored e-mail files or sending outgoing e-mail files, as both are web-based activities. *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1648 (2003). However, these types of web surfing activities are largely hidden from the user's perspective and typically do not require an independent surrendering of private information.

27 *See* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, SEC'Y ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973), *reprinted in* U.S. PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 15 n.7 (1977); *see also* Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 773 & n.9 (1999).

28 See *OECD*, Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, in OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 14-16 (Sept. 23, 1980), *available at* http://www1.oecd.org/publications/e-book/9302011E.pdf [hereinafter OECD Guidelines].

29 *Id.*

30 *Id.* at ¶ 19; OECD Guidelines, *supra* note 28, at National Implementation §§ 69-70.

oriented personal information by commercial websites on the World Wide Web.[31] With the implementation of the OECD's privacy guidelines, the United States has unequivocally chosen to center its website data collection privacy policy around information or database policy regulating the collection and use of personal information by commercial websites.[32]

The second issue is an individual's expectation of privacy in information stored in a computer. In determining whether an individual has a reasonable expectation of privacy in information stored in a computer, under a Fourth Amendment analysis, courts have consistently treated the computer like a closed container, such as a briefcase or a file cabinet. Such treatment adheres to information or database privacy.[33] The most basic Fourth Amendment question in computer cases asks whether an individual enjoys a reasonable expectation of privacy in electronic information stored within computers (or other electronic storage devices) under the individual's control, such as their laptop computers or floppy disks. As individuals generally retain a reasonable expectation of privacy in the contents of closed containers, they also generally retain a reasonable expectation of privacy in data held within electronic storage devices.[34] Accordingly, accessing information stored in a computer will ordinarily implicate an owner's reasonable expectation of privacy in the information.[35]

The last issue concerns the strict adherence to the category of information privacy protection that has been established in government-network service providers' relations, the searching and seiz-

---

31 *See* U.S. The FEDERAL TRADE COMMISSION ON "PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE" (2000), *available at* http://www.ftc.gov/os/2000/05/testimonyprivacy.htm#N_1_ (last visited Apr. 9, 2005). The FIPs have never been fully incorporated into U.S. law and merely remained a guiding source of law. For general discussion, see *supra* note 27 and Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575 (2003).

32 *See* Reidenberg, *supra* note 27, at 773-77 and accompanying notes (for the historical account in the U.S.).

33 The Fourth Amendment is not applicable to private website data collectors, including users, as "it is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official." United States v. Jacobsen, 466 U.S. 109, 113 (1984). Thus, the use of the Fourth Amendment "expectation of privacy" standard should be used in analogy, or as explained in context.

34 *See, e.g.*, United States v. Ross, 456 U.S. 798, 822-23 (1982).

35 *See* United States v. Barth, 26 F. Supp. 2d 929, 936-37 (W.D. Tex. 1998) (finding reasonable expectation of privacy in files stored on hard drive of personal computer); United States v. Reyes, 922 F. Supp. 818, 832-33 (S.D.N.Y. 1996) (finding reasonable expectation of privacy in data stored in a pager); United States v. Lynch, 908 F. Supp. 284, 287 (D.V.I. 1995) ; United States v. Chan, 830 F. Supp. 531, 535 (N.D. Cal. 1993); United States v. Blas, No. 90-CR-162, 1990 WL 265179, at *21 (E.D. Wis. Dec. 4, 1990) (analogizing expectation of privacy "in a pager, computer or other electronic data storage and retrieval device as in a closed container. . . .").

ing of computers, and the obtainment of electronic evidence. In particular, Congress embedded this policy in the Electronic Communications Privacy Act ("ECPA") of 1986,[36] which updated the Wiretap Act of 1968.[37] The ECPA regulates how the government can obtain stored account data in a computer,[38] or financial records and files,[39] from network service providers, such as ISPs, despite provisions protecting information privacy.[40] For example, the ECPA applies whenever agents or prosecutors seek stored e-mail, account records, or subscriber information from a network service.[41] Specifically, it expanded the coverage of the Wiretap Act by adding information or database privacy protection through Title 1,[42] which addresses the unauthorized interception of computer databases or electronic communication[43] while "in transit." It also expands coverage through Title 2,[44] which addresses the unauthorized acquisition of electronic communications while "in storage."[45] Overall, through several updates and expansions of the Wiretap Act, the ECPA became the predominant federal law protecting privacy through the category of information privacy in electronic and cyberspace communications from unauthorized interception, use, and disclosure in all private network service providers.[46] As mentioned above, this paper will focus on the first category of website data collection.

B. *Territorial Privacy: The Missing Category*

In some situations, the strict adherence to the category of in-

---

36 The Electronic Communications Privacy Act (ECPA), S. REP. No. 99-541, at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555 (codified as 18 U.S.C §§ 2510-2541 (1988)) (citing United States v. New York Tel. Co., 434 U.S. 159 (1977)).

37 *See* 18 U.S.C. §§ 2510-2521, §§ 2701-2710 (2000).

38 *See* 18 U.S.C. § 1030(1) (2000). Title 18 U.S.C. § 1030(e)(1) defines a computer as a data storage facility.

39 *See* 18 U.S.C. § 1030(a)(2)(a) (2000).

40 Other types of network service providers are telephone companies, cell phone service providers, and satellite services. *See* DEPARTMENT OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, at Introduction, *available at* http://www.cybercrime.gov/s&smanual2002.htm#_III_ (last visited Apr. 9, 2005) [hereinafter DOJ REPORT].

41 Title 18 U.S.C. §§ 2701-2712 creates statutory information privacy rights for customers and subscribers of computer network service providers; *see also* DOJ REPORT, at Part III.

42 *See* 18 U.S.C. §§ 2510-2521.

43 Electronic communications include telegraph, telex communications, electronic mail, non-voice digitized transmissions, and the portion of video teleconferences that do not involve the hearing of voice or oral sounds. *See* 18 U.S.C. § 2510(12).

44 *Id.*

45 Electronic storage includes computer random access memory, magnetic tapes, disks, and magnetic and optical media. *See* 18 U.S.C. §§ 2701-2710.

46 However, interception of communications made outside the United States is not within the scope of ECPA, while U.S. interstate communications "affecting interstate of foreign commerce" are included. *See* 18 U.S.C. § 2510(1).

formation privacy provides incomplete privacy solutions for website-related data collection practices. Arguably, in such situations, the integration of the category of territorial privacy should be justified in some analogy to physical world privacy protection. Largely put, the limitations of strictly adhering to the category of information privacy are fourfold and relate to the following: (1) the confusion concerning information privacy protection in multiple or mixed files; (2) the sequential and fast-moving usage of files in website navigation, as opposed to static data exchange in single databases; (3) the proprietary-based subject matter of the exception "available to the public" within its meaning in § 2511(2)(g)(i) of the ECPA; and (4) the added value of territorial segregation of on-line areas to the heterogeneity of data collection and consumer choice.

First, even though most courts accept the notion that electronic storage devices can be analogized to closed containers for Fourth Amendment purposes, they have reached contradictory conclusions over whether each digital file stored on a computer or disk should be treated as a separate closed container, subject to a single Fourth Amendment procedure. Thus, in some cases, certain courts have held that a computer disk containing multiple files is a single container. For example, in *United States v. Runyan*,[47] in which private parties had searched certain files and found child pornography, the Fifth Circuit held that the police did not exceed the extent of the private search when they examined supplementary files on any disk that had been, in part, privately searched.[48] Similarly, in *United States v. Slanina*,[49] the court held that when a warrantless search of a portion of a computer and zip disk had been justified, the defendant no longer retained any reasonable expectation of privacy in the remaining contents of the computer and disk; thus a comprehensive search by law enforcement personnel did not violate the Fourth Amendment.[50] However, these solutions do not suggest a coherent substantive legal policy.[51] In cases with similar circumstances, courts refused to comply with this broad interpretative approach. For example, in contradiction of

---

47 275 F.3d 449, 464-65 (5th Cir. 2001).

48 *Id.* at 464.

49 283 F.3d 670, 680 (5th Cir. 2002).

50 *Id.*

51 Although courts do see such multiplicity as a concerning phenomenon, as a procedural matter, however, evidence acquired from a network search that accessed data stored in multiple districts should not lead to suppression unless the agents intentionally and deliberately disregarded Rule 41(a) of the Federal Rules of Criminal Procedure, or prejudice resulted. *See generally* United States v. Trost, 152 F.3d 715, 722 (7th Cir. 1998).

the Fifth Circuit's approach, the Tenth Circuit has consistently refused to allow such exhaustive searches of a computer's hard disk in the absence of a warrant, or some exception to the warrant requirement.[52] The Tenth Circuit cautioned in one case, that "[b]ecause computers can hold so much information touching on many different areas of a person's life, there is greater potential for the 'intermingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer."[53]

Second, throughout the Internet, very large websites may be spread over a number of servers in different geographic locations.[54] IBM is a good example because its website consists of thousands of files spread out over many servers in world-wide locations, thereby defying the analogy between a file and a single container. Moreover, today, one can have multiple websites that cross-link to files on each others' sites or even share the same files.[55] These developments challenge even the Privacy Act's[56] broad file-based definition of a "record about an individual"—as "any item, collection, or grouping of information about an individual"[57]—for the case of large and complex websites. Arguably, this latter interpretative approach is becoming more acute, as the structure of websites and navigation through their files has become more sequential and fast-moving, as opposed to static data exchange in single files or databases.[58] Surfing speed, website, server complexity and size all increase navigation afforded by windows, menus, dialogue areas, control panels, etc. Thus, at least for large websites, this technological progress could imply a processional understanding of web navigation through sequences of content, as opposed to the earlier structural file search that is dominant in the

---

52 *See* United States v. Carey, 172 F.3d 1268, 1273-75 (10th Cir. 1999) (ruling that the agent exceeded the scope of a warrant to search for evidence of drug sales at the point where he "abandoned that search" and started searching for evidence of child pornography for five hours).

53 United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001).

54 A website is defined as a related collection of World Wide Web (WWW) files that includes a beginning file called a home page. *See* searchWebServices.com, *at* http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci541370,00.html (last visited Apr. 9, 2005).

55 *Id.*

56 5 U.S.C. § 552a (1994).

57 *Id.* at § 552a(a)(4). The Privacy Act, despite notable flaws, represents the most comprehensive attempt to structure information processing within the public sector but only applies to federal agencies.

58 *See* AARON MARCUS, PRINCIPLES OF EFFECTIVE VISUAL COMMUNICATION FOR GRAPHICAL USER INTERFACE DESIGN, READINGS IN HUMAN-COMPUTER INTERACTION 425-41 (Ron Baecker et al. eds., 2d. ed. 1995) [hereinafter MARCUS, PRINCIPLES OF EFFECTIVE VISUAL COMMUNICATION]; Aaron Marcus, *Metaphor Design in User Interfaces*, 22 ACM JOURNAL OF COMPUTER DOCUMENTATION 43, 43-57 (1998).

dissimilar physical world.[59]

Third, information privacy is also limited by the ECPA's privacy exception concerning files that are "available to the public" within its meaning in paragraph 2511(2)(g)(i).[60] This section permits "any person" to intercept an electronic communication made through a system "that is configured so that . . . [the] communication is readily accessible to the general public."[61] This exception has not yet been applied by the courts in any published cases concerning computers. This exception is primarily defined with respect to radio communications in the proposed section 210(16) of title 18.[62] Such 'public' communications would include the stereo subcarrier used in FM broadcasting or data carried on the VBI to provide closed-captioning of television programming for the hearing-impaired.[63] Thus, radio services readily accessible to the general public are exempt from this act's prohibitions against interception by the generic exception contained in paragraph 2511(2)(g)(i).[64]

Potentially, the statutory language could permit the interception of an electronic communication that has been posted to a public bulletin board, a public chat room, or a Usenet newsgroup.[65] Yet such an understanding of the paragraph is subject to several difficulties. First, the subject matter of that availability does not relate to a private place or locale, but to a file or a computer. Thus, the same difficulties described above remain present. Moreover, services that are available to the public are "remote computing services." As defined by § 2711(2), a service can only be a "remote computing service" if it is available "to the public" from a third party off-site computer that stores information for a customer.[66] This definition, therefore, does not deal with electronic communications that are not remote computing services, such as in the case of peer-to-peer communications, which are not technically prevented from containing files available to the public. In

---

59 MARCUS, PRINCIPLES OF EFFECTIVE VISUAL COMMUNICATION, *supra* note 58.

60 *See* 18 U.S.C. § 2511(2)(g)(i) (2000).

61 *Id.*

62 *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, S. REP. No. 99-541, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3572.

63 *Id.*

64 *Id.* at 3573.

65 *See* S. REP. No. 99-541, at 36 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3590 (discussing bulletin boards).

66 The term "remote computing service" ("RCS") means the provision to the public of computer storage or processing services by an off-site computer that stores or processes data for a customer. *See* S. REP. No. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3564-65. For example, a service provider that processes data in a time-sharing arrangement provides an RCS. *See* H.R. REP. No. 99-647, at 23 (1986).

addition, availability to the public within its meaning in § 2702(a), assumes that services comply with that definition if they are available to any user who complies with the requisite procedures and pays any requisite fees. Yet, the ECPA's definition of "public" excludes providers whose services are open only to those with a special relationship with the provider, such as employers who provide network accounts only to their employees.[67] Instead, a territorial privacy analysis may recognize public places even within privately provided websites,[68] overriding the proprietary-based dependency on baseline entitlements of services' owners and users.[69] Finally, the ECPA's present interpretation of availability "to the public" raises problems regarding the dependent definition of "intercept." For example, the seizure of a computer on which a private e-mail is stored, and which has been sent to an electronic bulletin board, but not yet read (retrieved) by the recipients, nevertheless constitutes an "intercept" proscribed by § 2511(1)(a).[70] In such a conflict, a territorially-based analysis would have maintained that even when control over the communication remains at the hand of the sender, the private communication nevertheless belongs to the public sphere. This is due to its mere location (once it has been posted), thus overriding the question of whether such communication was subsequently intercepted.[71]

Fourth, an on-line privacy policy that only supports the category of information privacy may only capture a sub-optimal value from segregation of heterogeneous on-line preferences. This argument is not unique to the Internet, but derives from Tiebout's well-known theorem, which all-purposely predicts that the further allo-

---

67 *See* Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998) (ruling that an internal e-mail system that was made available to a hired contractor, but was not available to "any member of the community at large," is excluded from the public).

68 For further analogy with the physical world with application to websites, see *infra* Part III.C.1.a.2.

69 *See* United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *2 (W.D. Wash. May 23, 2001) (ruling that defendant did not have a reasonable expectation of privacy in use of a private computer network when undercover federal agents looked over his shoulder and he did not own the computer he used). Nor will individuals generally enjoy a reasonable expectation of privacy in the contents of computers they have stolen. *See* United States v. Lyons, 992 F.2d 1029, 1031-32 (10th Cir. 1993).

70 *See* Steven Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 460 (5th Cir. 1994). In support of the general interception standard, see also United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997) ("[A]n e-mail message . . . cannot be afforded a reasonable expectation of privacy once that message is received."). *But see* C. Ryan Reetz, Note, Warrant Requirement for Searches of Computerized Information, 67 B.U. L. REV. 179, 200-06 (1987) (arguing that certain kinds of remotely stored computer files should retain Fourth Amendment protection, and attempting to distinguish *United States v. Miller*, 424 U.S. 435 (1976) and *Smith v. Maryland*, 442 U.S. 735 (1979)).

71 For further analogy to the physical world and its application to websites, see *infra* Part III.C.1.A.

cation of legal rights to different types of territorial locales would exercise strong effects upon the heterogeneity of data collection practices.[72] This loss of value already results due to the fact that distinct data collection practices and consumer navigation choices are prevented from complementing territorially-based segregation. In the physical world, Tiebout's model is perceived to be widely successful in predicting the demand curve economic causes of urban spatial segregation due to inter-jurisdictional competition.[73] To date, Tiebout's model serves as the basis for the justification of contemporary system state-based corporate regulation.[74] Tiebout states that "spatial mobility provides the local public goods counterpart to the private market's shopping trip."[75] Tiebout's rationale points to a clustering effect in which users of very similar demands for the local public good naturally would then choose to subsist in the same on-line community.

Tiebout's model may apply even more efficiently in cyberspace where there are zero transaction cost. Tiebout explains that perfect competition between jurisdictions can only occur if citizens have complete information and if mobility between jurisdictions is costless.[76] Using a system of a decentralized provision of public good, such as privacy through self-regulated website owners, consumers would be required to reveal their more advanced prefer-

---

72 *See* Charles M. Tiebout, *A Pure Theory of Local Expenditures*, 64 J. POL. ECON. 416 (1956) (for a hypothesis of consumer-voters sorting themselves based on preferences for a package of taxes, services, and amenities); *see also* Otto A. Davis & George H. Haines, Jr., *A Political Approach to a Theory of Public Expenditure: The Case of Municipalities*, 19 NAT'L TAX J. 259, 260 (1966).

73 *See* William W. Bratton & Joseph A. McCahery, *The New Economics of Jurisdictional Competition: Devolutionary Federalism in a Second-Best World*, 86 GEO. L.J. 201, 205-06 (1997). For supporting surveys, see THOMAS M. SMITH ET AL., U.S. DEP'T OF EDUC., THE CONDITION OF EDUCATION 1997 23 (1997) (reporting results of the National Household Education Survey, in which approximately 50% of parents whose children attended neighborhood schools claimed that "their choice of residence was influenced by where their children would go to school."). *See also* Kenneth N. Bickers & Robert M. Stein, *The Microfoundations of the Tiebout Model*, 34 URB. AFF. REV. 76, 88 (1998) (reporting survey results which indicated that 92% of respondents with school-age children stated that "the quality of schools is important or very important in influencing their decision" of where to live); F.J. Calzonetti & Robert T. Walker, *Factors Affecting Industrial Location Decisions: A Survey Approach*, *in* INDUSTRY LOCATION AND PUBLIC POLICY 221 (Henry W. Herzog, Jr. & Alan M. Schlottmann eds., 1991); Henry W. Herzog, Jr. & Alan M. Schlottmann, *Metropolitan Dimensions of High-Technology Location in the U.S.: Worker Mobility and Residence Choice*, *in* INDUSTRY LOCATION AND PUBLIC POLICY, *supra*, at 169, 176-77.

74 *See, e.g.*, ROBERTA ROMANO, THE GENIUS OF AMERICAN CORPORATE LAW (1993) (justifying federalism per its ability to generate competition among states); John D. Donahue, *Tiebout? Or Not Tiebout? The Market Metaphor and America's Devolution Debate*, 11 J. ECON. PERSP. 73, 74 (1997); Richard Epstein, *Exit Rights Under Federalism*, 55 LAW & CONTEMP. PROBS. 147 (1992); Michael W. McConnell, *Federalism: Evaluating the Founders' Design*, 54 U. CHI. L. REV. 1484, 1491-1511 (1987).

75 Tiebout, *supra* note 72, at 422.

76 *Id.* at 418.

ences for different amounts of privacy. Such a regime would be a reflection of their personal privacy demand curves in whole websites or separate areas within them. Such segregated on-line territorial areas would then be backed by different territorial privacy policies, specifically private and public, competing with website owners offering only information privacy or a combination of the two. This would, justify the geographical variation of on-line privacy rules.

The added value from on-line territorial privacy must be carefully considered. As will be explained later, it would legitimate observance and non-identifiable data collection in an on-line public locale, or in a locale that may be viewed from a public one. Notably, with regard to databases, much information collection and use occurs in what would otherwise be considered public and, indeed, many parts of cyberspace may well be considered public locales.[77] For example, a chat room can technically be maintained as either a website or as part of a website.[78] Nevertheless, with lack of sufficient clarity, even potential public locales, such as chat rooms, are presently under-regulated and lack privacy policy precision.[79]

The absence of self-regulation, or new legislation integrating territorial privacy, already brings into question the extent to which website owners will seek to shield themselves from liability for deceptive practices as a result of not establishing a coherent privacy policy in the first instance. The FTC's enforcement action against GeoCities highlights the leaky privacy protection offered by websites.[80] GeoCities markets itself as a "virtual community" that or-

---

[77] *See, e.g.*, Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1433 (2001); *see also* discussion *infra* Part III.B.2.

[78] *See* searchWebServices.com, *Chat Room, at* http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci541370,00.html (last visited Apr. 9, 2005).

[79] *See* America Online, Inc., *AOL Instant Messenger Web Chat Rules & Etiquette, at* http://www.aol.com/community/rules.html (last visited Apr. 9, 2005) (containing a murky list of web chat rules and etiquette:

> When communicating in a chat room be mindful that many people will be able to view it and the inclusion of information such as your name, your address or telephone number is never recommended . . . It's also a good rule-of-thumb to check the Privacy Policies of any unfamiliar or new web sites you visit);

see also America Online, *Privacy Policy, at* http://www.aol.com/info/privacy.adp (last visited Apr. 9, 2005) (ignoring the public nature of chat rooms, while over inclusively stating "This privacy policy applies to the AOL.com site."); Yahoo!, *Privacy Policy, at* http://privacy.yahoo.com (last visited Apr. 9, 2004) (same, but applying to the Yahoo.com site); United States v. Charbonneau, 979 F. Supp. 1177 (S.D. Ohio 1997) (denying a reasonable expectation of privacy in a chat room providing that defendant is made aware of the operating procedures in that chat room); United States v. Maxwell, 45 M.J. 406, 419 (C.A.A.F. 1996) (mentioning in dicta "[m]essages sent to the public at large in the 'chat room' . . . lose any semblance of privacy.").

[80] *See* GeoCities Proposed Consent Agreement, 63 Fed. Reg. 44,624 (Fed. Trade Comm'n Aug. 20, 1998) (final approval Feb. 12, 1999). The GeoCities Consent Order could also be found at www.ftc.gov/opa/1998/9808/geocitie.htm (no longer available on-

ganizes its members' home pages into forty different areas, termed "neighborhoods." In these areas, members can post a personal Web page, receive e-mail, and participate in chat rooms. Non-members can also visit many areas of GeoCities. According to the FTC, GeoCities engaged in two kinds of deceptive practices in connection with its collection and use of personal information. First, although GeoCities promised a limited use of the data it collected, it in fact sold, rented, and otherwise disclosed this information to third parties who used it for purposes well beyond the scope of permission given by individuals. However, at no point was this practice recognized in what would have been otherwise acknowledged as GeoCities's public locale. Second, GeoCities promised that it would be responsible for the maintenance of the data collected from children in the "Enchanted Forest" part of its website. Instead, it turned such personal information over to third parties called "community leaders." That activity could have been made legitimate by allowing the construction of that part of its website as public. Finally, GeoCities settled with the FTC and promised to make significant changes in its privacy practices.[81] The final order permits GeoCities to collect or use personal data about children to the extent permitted by the Children's Online Privacy Protection Act of 1998.[82] Again, this ignores the possibility of recognizing a separate territorial privacy policy, fencing out the public part of its website.

Nevertheless, the value of integrating on-line territorial privacy is not comparable for all types of data collected. Currently, there are two basic ways used by websites to collect such "non-content" personal information.[83] The first is by directly collecting information from users ("Registration" and "Transactional" data).[84] Regis-

---

line) and a FTC discussion could be found at Analysis of Proposed Consent Order to Aid Public Comment, at www.ftc.gov/os/1998/9808/9823015.ana.htm (no longer available on-line). The GeoCities website is located at http://www.geocities.com (last visited Apr. 9, 2005). The FTC was able to obtain jurisdiction in this case only because GeoCities' false representations regarding its privacy practices constituted "deceptive acts or practices" under the Federal Trade Commission Act.

81 *See* GeoCities Proposed Consent Agreement, 63 Fed. Reg. 44,624; FTC, Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case, *at* www.ftc.gov/opa/1998/9808/geocitie.htm (last visited Apr. 9, 2005).

82 *See* Jeffrey P. Cunard et al., *Communications Law* 1999, 581 P.L.I. PAT 853 (Nov. 1999).

83 There are also "contents" within its' meaning at 18 U.S.C. §§ 2510(8), 2703(c)(1) (2000) of the ECPA. The contents of a network account are the actual files stored in the account. *See* 18 U.S.C. § 2510(8). However, in practice, website owners do not typically collect "contents." Alternatively, this type of data collection may limit users' "communications privacy," whenever it is collected by other users. *See supra* Part I.A. For further explanation, see discussion herein.

84 *See* Solove, *Privacy and Power*, *supra* note 77, at 1411.

tration data is collected by those websites that request users to login in order to access parts of the website. In reference to the ECPA's definitions, registration data can be seen as "basic subscriber information" according to 18 U.S.C. § 2703(c)(2).[85] A second type of data that is collected directly by websites is transactional data. It is "gleaned by websites engaging in business with users, such as selling merchandise or services."[86] In reference to ECPA § 2703(c)(1), transactional data relates to "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)." The broad definition of this category seems to comprise of all records that are not contents, including basic subscriber information.

The second way through which websites collect data is indirect. This is done by tracking the way people navigate through the Internet ("Clickstream" data), which "enables the website to calculate how many times it has been visited and what parts are the most popular."[87] It may also be seen to include information revealed by uniquely distinguishing features of a user's computer, such as the unique serial numbers contained in Intel's Pentium III chips.[88] As this study argues, database protection against such forms of information collection, particularly registration data that is collected upon initial entry to databases, is an overly generalized, and thus over-inclusive, privacy category.[89] It implicitly includes both possible public and private on-line locales, while overly protecting the former.

---

85 Title 18 U.S.C. § 2703(c)(2) (2000) lists the categories of basic subscriber information: (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number). In general, the items in this list recount the identity of a subscriber, but for ECPA's purposes, also her association with her Internet service provider ("ISP") and her basic session connection records. The Patriot Act enhanced the categories of basic subscriber information in three respects. *See* Patriot Act § 210, 115 Stat. 272, 283 (2001). It added "records of session times and durations," as well as "any temporarily assigned network address" to 18 U.S.C. § 2703(c)(2). Lastly, the Patriot Act added the "means and source of payment" that a customer uses to pay for an account, "including any credit card or bank account number."

86 Solove, *supra* note 77, at 1411.

87 *Id.*

88 *See* MICHIGAN LAW REVISION COMMISSION, PRIVACY AND THE INTERNET: A STUDY REPORT TO THE MICHIGAN LAW REVISION COMMISSION, MICHIGAN LAW REVISION COMMISSION THIRTY-FIFTH ANNUAL REPORT 15 (2000), *available at* http://www.milegislativecouncil.org/mlrc/2000/PrivacyandInternet.htm (last visited Apr. 9, 2005).

89 Definitions of database or equivalent terms in proposed U.S. legislation, such as the Consumer and Investor Access to Information Act of 1999, H.R. 1858, 106th Cong. § 101(1) (1999), have been a little more detailed. *See* Jacqueline Lipton, Balancing *Private Rights and Public Reconceptualizing Property in Databases*, BERKELEY TECH. L.J. 773 (2003).

Finally, on-line territorial privacy, arguably, should not categorically replace on-line information privacy. Instead, whenever necessary and possible, it should complement it. In the physical world, courts have rejected cases involving territorial intrusion whenever the privacy infringement was done in databases and would therefore belong to the category of information or database privacy. This includes the rejection of obtaining a person's unlisted phone number,[90] the selling of subscription lists to direct mail companies,[91] or the collection and disclosure of an individual's past insurance history.[92] Therefore, constructing a similar balance per se within cyberspace would not be unprecedented.

C. *Constructing On-line Territoriality: The Argument's Structure*

Analogous to the physical world, the suggested adaptation of territorial privacy to cyberspace based on the tort of intrusion upon seclusion will overcome many of these anomalies. Notably, it would prevail over the jurisprudential obstacles left by the doctrine of trespass to chattels that is commonly referred to in access policy cases in cyberspace.[93] Particularly, territorial privacy and private and public locales could coexist on the Internet, just as they do in the physical world.[94] Courts would then be required to differentiate and identify public locales and then separate them from private ones. Thus far, cyberspace has not been left with public locales, nor has a balanced territorial privacy policy been established. Instead, only a *private* and overly broad privacy legal rule has been adopted. In continuation of previous jurisprudential developments, privacy should continue to be revalued instrumentally.[95]

---

90 *See* Seaphus v. Lilly, 691 F. Supp. 127, 132 (N.D. Ill. 1988).

91 *See* Shibley v. Time, Inc., 341 N.E.2d 337, 339 (Ohio Ct. App. 1975).

92 *See* Tureen v. Equifax, Inc., 571 F.2d 411, 416 (8th Cir. 1978).

93 Under the alternative doctrine of trespass to chattels, an actor can commit a trespass to chattels by using, or intermeddling with, a chattel only if it is in the possession of another. *See* RESTATEMENT (SECOND) OF TORTS § 217(b) (1965); *see also* Curtis J. Berger, *Pruneyard Revisited: Political Activity on Private Lands*, 66 N.Y.U. L. REV. 633, 655 (1991) (similarly arguing for the physical world). Furthermore, while trespass to chattels can represent the civil branch of the unauthorized access cases, it does not focus on the privacy of the data subject per se. Rather, it focuses on the concept of intrusion into a protected area that is different than access to the data subject or appropriation of the information gathered. *See, e.g.*, Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 26-41, 61 (1996). For further analysis, *see* discussion *infra* Part III.

94 *See, e.g.*, Carol M. Rose, *The Several Futures of Property: Of Cyberspace and Folk Tales, Emissions Trades and Ecosystems*, 83 MINN. L. REV. 129, 154 (1998); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607 (1999) (adding to public and private locales the quasi-public locale). Notwithstanding the importance of quasi-public locales, and in compliance with general tort of intrusion jurisprudence, I will ignore this latter category.

95 *See* Solove, *supra* note 10, at 1144-1145; INNESS, *supra* note 1, at 95. One example is

Ultimately, a legal fiction of on-line locales should now be constructed for cyberspace's overall privacy policy.[96] For such a legal fiction to be effectively applicable and harmonious with privacy protection at large, a comprehensive boundary framework for cyberspace must be agreed upon, as explained in Parts II-VI below.

Part II provides an overview of the two competing boundary approaches for cyberspace. Cyberspace is still arguably left without a comprehensive boundary approach, and courts or legislators have not yet been successful in collectively adopting one. However, in theory, cyberspace boundary discourse is nevertheless present. It has given rise to two conflicting approaches, referred to herein as the "globalist" approach and the "anti-globalist" approach, while largely ignoring the more sensible legal alternative—one based on a "localist" boundary approach, which will be critically assessed in this part.

The globalist boundary theory is a rather optimistic technologically-oriented analysis, which suggests that cyberspace is bound to be zoned similarly to the physical world. However, according to Lessig and Shapiro, separate on-line spatiality does not exist or that, and according to Johnson and Post, spatiality exists separately from the physical world and might allow some degree of zoning. In both ways, as argued, spatiality is seen merely as a technological constraint that could override the legal understanding of spatiality. In essence, both are looking for a technological solution and underestimate the role of law in erecting boundaries in cyberspace. Therefore, both uphold two competing versions of a globalist boundary theory for cyberspace. The second approach could be seen as an antithesis to the globalist approach, in the face of an anti-globalist boundary theory for cyberspace. Among its supporters are Hunter, Lemley, and others who also focus their spatial analysis on the technological regulative constraint. Their message largely rejects the spatial analogy between the physical space and

---

the Court's 1928 decision in Olmstead v. United States, 277 U.S. 438 (1928), which epitomized the need for interpretive flexibility in constructing privacy. The Court held that the wiretapping of a person's home telephone (done outside a person's house) did not run afoul of the Fourth Amendment because it did not involve a trespass inside a person's home. *Id.* at 465. It was not until 1967 that the Court in Katz v. United States, 389 U.S. 347 (1967), overruled *Olmstead*, and held that wiretapping does not necessitate physical trespass. *See* Carl Shapiro & Hal R. Varian, *U.S. Government Information Policy* 45 (July 30, 1997), *available at* http://www.sims.berkeley.edu/~hal/Papers/policy/policy.html#SECTION00081000000000000000 (last visited Apr. 9, 2005).

96 *See generally* Andrew L. Shapiro, *Street Corners in Cyberspace: Free Public Forums Must be Preserved on Internet*, THE NATION, July 3, 1995, at 10 (in justification of the First Amendment "public forum" doctrine); David J. Goldstone, *A Funny Thing Happened on the Way to the Cyber Forum: Public v. Private in Cyberspace Speech*, 69 U. COLO. L. REV. 1, 3 (Winter 1998). For further explanation, see discussion herein.

cyberspace because, according to these scholars, cyberspace is not a real "place," but instead is a medium where tangible objects do not exist.[97]

Geared with the motivation to find and legalize their underlying scientific truths, both the globalist and anti-globalist approaches share a tendency to make the law overly scientistic in those instances when science and law interact, as then can be applied through the case of on-line territorial privacy protection. In addition, both approaches do not seem to have appropriately dealt with challenges to their scientific or hypothetical truths, which they assume, nor do they seem to have adequately confronted the constructive legal implications of an altogether contending localist boundary theory for cyberspace. Legal truth about cyberspace spatiality should then be a tentative scientific truth, transformed from mere particular scientific truths backed by legal values, to an inclusive legal truth by courts or other regulating institutions.

Still, it should be noted that Anglo-American jurisprudence has a long history of viewing factual or scientific truth as only one parameter in establishing legal truth. Therefore, the factual or scientific validity of spatial or non-physical boundaries should not inherently serve as a binding constraint on a possible legal formation of on-line locales. Area or local differentiation should now replace the homogenous spatial organization as the major conceptual focus of cyberspace's globalist boundary theory. Consequently, the allocation of legal rights to different types of locales, predominantly private and public, would then exercise strong effects upon the heterogeneity of data collection practices. This would justify the geographical variation of on-line privacy rules.

Part III asserts that the law may indeed construct a legal fiction of on-line locales without committing itself to their global continuous spatial organization. Seen through the prism of the cumulative characteristics of legal fictions, this part confronts both globalist and anti-globalist boundary rationales in support of the comprehensive theoretical structure of localist boundary application to the law at large. Ultimately, this part applies the construction of a legal fiction of on-line locales to territorial privacy as part of cyberspace's overall privacy policy.

Part IV advances several policy rationales concerning the pros-

---

97 *See, e.g.*, Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439, 472 (2003); Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521, 523 (2003); Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U. CHI. LEGAL F. 217, 217; Maureen A. O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 BERKELEY TECH. L.J. 561, 567 (2001).

pect of integrating territorial privacy in cyberspace. It concludes by suggesting that, notwithstanding the category of information privacy protection, territorial privacy in cyberspace's private and public locales could coexist on the Internet in much the same way as it does in the physical world. Courts would then be required, first, to differentiate and identify public locales and then, second, to fence them out from private ones.

I. CYBERSPACE BOUNDARY DISCOURSE: THE TWO APPROACHES

In the quest for exercising regulatory or judicial jurisdiction in the physical sphere, the Anglo-American legal system traditionally requires the establishment of a "geographic nexus"—the connection required to give an individual or government a legitimate interest in a legal controversy in a given "locale."[98] In terms of political geography, it is largely agreed that any boundary theory consists of the attributes of such locales in space (points, lines, or areas) and the interactions, or nexus, between these locations.[99] In this sense, space is the conceptualization of the imagined physical relationships which give meaning to society.[100] Locale, on the other hand, is the distinct space that encompasses both the idea and the actuality of where things are.[101] Referring to the nested hierarchy of bounded spaces of differing size, such as local, regional, national, and global, is a familiar and taken-for-granted concept of political geographers and political analysts.[102] Numerous scholars have employed a framework that utilizes three scales of analysis: international or global, national or state level, and an intra-national, which is usually an urban metropolitan scale.[103] These are relatively closed and self-sufficient systems.[104]

Also incorporated into the physical world's legal discourse are

---

98 *See, e.g.*, Daniel A. Farber, *Stretching The Margins: The Geographic Nexus in Environmental Law*, 48 STAN. L. REV. 1247, 1273-75 (1996) (in application to international environmental law); Christopher D. Stone, *Locale and Legitimacy in International Environmental Law*, 48 STAN. L. REV. 1279 (1996).

99 For matters of convenience, the terms "locale" and "location" will be used interchangeably. *See* Edward W. Soja, *A Paradigm for the Geographical Analysis of Political Systems*, *in* LOCATIONAL APPROACHES TO POWER AND CONFLICT 53-71 (Kevin R. Cox et al. eds., 1974); R.J. JOHNSON, SPATIAL STRUCTURES 14 (Mathuen 1973); HENCE SHORT, AN INTRODUCTION TO POLITICAL GEOGRAPHY 1 (Routledge & Kegan Paul 1982); DAVID DELANEY & HELGA LEITNER, *The Political Construction of Scale*, 16 POLITICAL GEOGRAPHY, NO. 2, 93 (1997).

100 *See* M. KEITH & S. PILE, PLACE AND POLITICS OF IDENTITY (1993); A. Gupta, *Blurred Boundaries: The Discourse of Corruption, The Culture of Politics, and the Imagined State*, 22 AMERICAN ETHNOLOGIST No. 2, 375-402 (1992).

101 *See* Gupta, *supra* note 100, at 375-402.

102 *See* DELANEY, *supra* note 99, at 93.

103 *See, e.g.*, PETER TAYLOR, POLITICAL GEOGRAPHY: WORLD-ECONOMY, NATION-STATE AND LOCALITY 43, 44 (1993).

104 JOHNSON, *supra* note 99, at 14.

the two main competing interpretive border theories thus far developed: a globalist and a localist. Each, as will be explained, is insufficiently attentive to the values represented by the other.[105] They pivot around the basic unit of the state, hence the international, national, and intra-national terminology.[106] The first is a "spatial" analysis, which refers to globalist boundary theory that has been adopted in international, environmental, and even criminal law. Globalism gives every government an equally legitimate concern with every issue without offering any line drawing rationale; in that sense, it attempts to erase geographic discontinuity. The basic idea of globalism is that legal controversies know no territorial boundaries.[107] What happens in one place affects everyone everywhere, and no particular geographic nexus should be required as a basis for legal action.[108] According to the globalist approach, geographical uniformity is not an inevitable feature of a legal rule.[109]

The second is an "areal" analysis, which refers to localist boundary theory. Localism tends to place talismanic weight on physical location and presence as its core concern.[110] At the international level, localism is surely the baseline.[111] An individual physically present in a locale has a cognizable interest in it, just as governments have a legitimate interest in threats that are physically present within their territories.[112] The perception that objective physical conditions vary from locale to locale may then lead rule makers to pursue a consistent and comprehensive legal policy by adopting different localized legal rules, based on respective distinctive jurisdictions. Thus far, cyberspace is still left without a comprehensive boundary approach, and courts and legislators have failed to adopt one. However, in theory, cyberspace boundary discourse is nevertheless present, and has given rise to two conflicting approaches—a globalist and anti-globalist—while largely ignoring the

---

105 HASTINGS DONNAN & THOMAS M. WILSON, BORDERS: FRONTIERS OF IDENTITY, NATION AND STATE 9 (1999); Farber, *supra* note 98, at 1247-48, 1270-71 (investigating the conflict between localist and global perspectives in environmental law); Edward Soja, *Surveying Law and Borders: Afterword*, 48 STAN. L. REV. 1421, 1426 (1996) (same) [hereinafter Soja, *Surveying Law and Borders*]; Soja, *supra* note 99, at 53.

106 *See, e.g.*, TAYLOR, *supra* note 103, at 44.

107 *See also* Digital Equip. Corp. v. Altavista Tech., Inc., 960 F. Supp. 456, 462 (D. Mass. 1997) (stating for the context of cyberspace "[t]he Internet has no territorial boundaries."). For further analysis, see discussion *infra* Part II.A.

108 *See* Farber, *supra* note 98, at 1272.

109 *See* Gerald L. Neuman, *Surveying Law and Borders: Anomalous Zones*, 48 STAN. L. REV. 1197, 1201 (1996).

110 *See* Farber, *supra* note 98, at 1270; Soja, *supra* note 99, at 53.

111 *See* Farber, *supra* note 98, at 1270; Soja, *supra* note 99, at 53.

112 *See* Farber, *supra* note 98, at 1270; Soja, *supra* note 99, at 53.

more sensible legal alternative, one based on a localist boundary approach, which will be critically assessed herein.

The regulative debate regarding the question of spatiality in cyberspace has primarily presented contradicting approaches towards globalist boundary theory. The first is a basic globalist boundary approach. Its rather optimistic, technologically-oriented analysis suggests that cyberspace should be zoned similarly to the physical world. However, separate on-line spatiality does not exist, according to notable scholars like Lessig or Shapiro, although according to Johnson and Post, spatiality exists separately and might allow some degree of zoning. In both ways, spatiality is merely seen as a technological constraint that overrides any legal definition of spatiality. Thus, in agreement with Johnson and Post, Lessig predicts that in cyberspace, the game is becoming code, thereby rendering law a sideshow. Such technological primacy is more than a difference in efficiency.[113] In essence, both sets of scholars are looking for a technological solution which arguably underestimates the role of law. Overall, both uphold two competing versions of a globalist boundary approach for cyberspace. The second approach stands as an antithesis to the former and could be seen as an anti-globalist boundary approach. Among its supporters are Hunter, Lemley, and others who also focus their spatial analysis on the technological regulative constraint. Nevertheless, their rather skeptical inclination is to argue that technology has, in fact, failed to create substantive on-line spatiality and nothing can be put in its place. As will be described briefly herein, both the globalist and the anti-globalist approaches alike do not seem to have appropriately dealt with challenges to the underlying scientific or hypothetical truths which they assume. They also do not seem to have adequately confronted the constructive legal implications of a contending localist boundary theory for cyberspace.

A. *Globalist BoundaryTheory: Johnson & Post and Lessig*

Until the digital era, there was a general correspondence between borders drawn in physical space (between nation-states or other political entities) and their conceptual definitions in what Johnson and Post allegorically call "law space."[114] Nowadays, cyberspace is dealing with a genuine fencing challenge with "law space,"

---

113 *See* LAWRENCE LESSIG, THE CONSTITUTION OF CODE: LIMITATIONS ON CHOICE—BASED CRITIQUES OF CYBERSPACE REGULATION 181-82 (1997); LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 130 (Basic books 1999).

114 *See* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1368 (1996).

or more simply, law needing to correspond to non-physical jurisdictions. Consequently, cyberspace is experiencing a conflict between different boundary theory traditions that affects its culture and development.[115] Thus far, application of cyberspace globalist boundary theory notably focuses *not* on whether fencing in or fencing out is more appropriate for some aspect of cyberspace, but whether there could and should be fences at all. It also focuses on whether law has the legitimacy to erect them.

In compliance with the acute technologically-oriented approach that focuses on the technological reality as the main constraint, courts seem to have generally followed this technocentristic line of argumentation. That choice was ultimately encapsulated in the case of *Reno v. ACLU*,[116] where the Court concluded that the Internet was deserving of full First Amendment protection, not the lesser protection afforded to broadcast media. In doing so, the Court considered how well each metaphor actually applied in cyberspace. The Court concluded that cyberspace allowed the construction and use of barriers to screen for identity, making cyberspace more like the physical world and, consequently, more amenable to zoning laws.[117] Justice O'Connor's concurrence makes that very controversial assumption by observing that "[c]yberspace undeniably reflects some form of geography; chat rooms and Web sites, for example, exist at fixed 'locations' on the Internet."[118]

Nevertheless, the major difficulty with this strict comparison between cyberspace and the physical world is the line of argument which suggests that the aggregate existence of distinctive locales implies a globalist boundary notion of continuous spatiality, whether in connection with the physical world or not. In other words, if we recognize that cyberspace is constituted by locales in which a variety of interactions may occur, one must think about the spatial relationship among them.

This technologically oriented view of at least physical-virtual continuous spatiality, upheld by the Supreme Court, has also gained popularity among the academic community. The works of

---

115 *See* Jonathan J. Rusch, *Cyberspace and the "Devil's Hatband"*, 24 SEATTLE U. L. REV. 577, 585, 591-92 (2000).

116 *See* 521 U.S. 844 (1997).

117 *Id.* at 891.

118 *See id.* at 886 (O'Connor, J., concurring in the judgment in part and dissenting in part). For opposing opinions in several lower court decisions, see, for example, American Libraries Ass'n v. Pataki, 969 F. Supp. 160, 168-69 (S.D.N.Y. 1997), where the court found that "geography, however, is a virtually meaningless construct on the Internet," and Digital Equipment Corp. v. Altavista Technology, Inc., 960 F. Supp. 456, 462-63 (D. Mass. 1997).

Lawrence Lessig, Andrew Shapiro, Trotter Hardy, and others, are perhaps those that most paved the way in that direction. In harmony with the Court's continuity choice, and unlike Johnson and Post who argue for a separation between real space law and cyberspace law, Lessig does not believe such separation can be sustained, nor that it should be.[119]

Lessig places much faith in technology at the expense of a weakened legal approach. He argues that "what is missing in discourse about Cyberspace and its regulation is a richer understanding of the range of architectures that are possible."[120] The architecture of cyberspace, we are told, will in principle allow for perfect zoning, a way to perfectly exclude those who would cross boundaries.[121] Advances in technology, not law, will make zoning the Internet feasible in the future.[122]

Overall, Lessig, Hardy, and others agree that zoning will replace the present wilderness of cyberspace, thereby implicitly adhering to a globalist boundary approach in cyberspace that is in concert with Johnson and Post. In this spatial realm where technology is king, zoning will be achieved through code—a tool, as Johnson and Post suggest, more perfect than any equivalent tool of zoning in real space.[123] In further recognition of a spatial approach to cyberspace, it is probably the case that the cost of both drawing borders (identifying digital information as one's own) and monitoring border trespasses (detecting unauthorized copying or alterations) seem to be no higher in cyberspace than they are for real property.[124] Such costs may even be lower in cyberspace thanks to recent technological developments.[125]

In opposition to Lessig's view regarding a continuous physical-virtual spatiality, lies a competing globalist boundary approach, which suggests that spatiality in cyberspace is, in fact, separate from that of the physical world. This view, as well, upholds a strict tech-

---

119 *See* Lawrence Lessig, *The Zones of Cyberspace*, STAN. L. REV. 1403, 1403 (1996); *see also* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999); Andrew L. Shapiro, *The Disappearance of Cyberspace and the Rise of Code*, 8 SETON HALL CONST. L.J. 703, 704, 714-15 & n.29 (1998); Soja, *supra* note 105, at 1427. For earlier observations, see also M. Ethan Katsh, *Rights, Camera, Action: Cyberspatial Settings and the First Amendment*, 104 YALE L.J. 1681, 1686 (1995) (referring to JOSHUA MEYROWITZ, NO SENSE OF PLACE: THE IMPACT OF ELECTRONIC MEDIA ON SOCIAL BEHAVIOR 38 (1985)) (physical settings and media "settings" are part of a continuum rather than a dichotomy).

120 Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 65 (1999).

121 *See* Lessig, *Zones of Cyberspace*, *supra* note 119, at 1409.

122 *See* Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 886-901 (1996).

123 *See* Lessig, *Zones of Cyberspace*, *supra* note 119, at 1409.

124 *See* Hardy, *supra* note 97, at 259.

125 *Id.*

nologically-centered approach, while suggesting that spatiality is mostly a technological concern.[126]

The leaders of this alternative libertarian orthodoxy are David Post and David Johnson.[127] Their major explicit globalist premise is that cyberspace is a space, or has the characteristics of a space, in disconnection from physical space.[128] As they suggest, many of the jurisdictional and substantive quandaries raised by border-crossing electronic communications could be resolved by one simple principle: cyberspace should be conceived as a distinct space for purposes of legal analysis by recognizing a legally significant border between cyberspace and the physical world.[129] On a normative level, their line of thinking then argues against the adaptation of "geographic legal space" to "cyber space or spaces." We are told that traditional legal reasoning is not only secondary in constraining behavioral preferences on-line, but potentially disruptive. Consequently, because there are no physical locales, there should not be "legal" ones.[130] Thus, any insistence on "reducing" all on-line transactions to a legal analysis based in geographic terms presents a new "mind-body" problem on a global scale.[131]

As a legal matter, an original globalist border theory approach to cyberspace treats cyberspace as a separate "space" to which the application of distinct sets of laws should come naturally.[132] Therefore, we must either refrain from applying these ineffective real-

---

126 *See, e.g.*, Lawrence Lessig & Paul Resnick, *Zoning Speech on the Internet: A Legal and Technical Model*, 98 MICH. L. REV. 395, 396 (1999); Lawrence Lessig, *The Death of Cyberspace*, WASH. & LEE L. Rev. 337, 344 (2000).

127 *See* Johnson & Post, *supra* note 114, at 1379; David R. Johnson, *"Chaos Prevailing on Every Continent": Towards a New Theory of Decentralized Decision-Making in Complex Systems*, 73 CHI.-KENT L. REV. 1055 (1998); David G. Post, *Governing Cyberspace*, 43 WAYNE L. REV. 155, 161 (1996).

For early libertarian literature on the matter, see John Perry Barlow, *Is There a There in Cyberspace?*, at http://www.eff.org/Misc/Publications/John_Perry_Barlow/HTML/utne_community.html (last visited Apr. 9, 2005). *See also* Esther Dyson et al., *Cyberspace and the American Dream: A Magna Carta for the Knowledge Age* (Aug. 22, 1994), *at* http://www.pff.org/issues-pubs/futureinsights/fi1.2magnacarta.html (last visited Apr. 9, 2005); Mitchell Kapor & John Perry Barlow, *Across the Electronic Frontier* (July 10, 1990), *in* ROBERT B. GELMAN & STANTON MCCANDLISH, PROTECTING YOURSELF ONLINE: THE DEFINITIVE RESOURCE ON SAFETY, FREEDOM, AND PRIVACY IN CYBERSPACE 14 (1998), *available at* www.eff.org/Misc/Publications/John_Perry_Barlow/HTML/eff.html.

128 *See* Johnson & Post, *supra* note 114, at 1379, 1381.

129 *Id.* at 1378.

130 *Id.* at 1370-72; *see, e.g.*, Dan L. Burk, *Federalism in Cyberspace*, 28 CONN. L. REV. 1095, 1098-99 (1996); Michael Froomkin, *The Internet as a Source of Regulatory Arbitrage*, *in* BORDERS IN CYBERSPACE 129, 142-55 (Brian Kahin & Charles Nesson eds., 1997); Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, *in* BORDERS IN CYBERSPACE 84, 86-87 (1996); Henry H. Perritt, Jr., *Jurisdiction in Cyberspace*, 41 VILL. L. REV. 1, 100-03 (1996) (supporting the "United States District Court for the District of Cyberspace").

131 *See* Johnson & Post, *supra* note 114, at 1378.

132 *See id.* at 1379; *see also* David Johnson & David Post, *And How Shall the Net Be Governed? A Meditation on the Relative Virtues of Decentralized, Emergent Law*, *in* COORDINATING THE IN-

space laws to cyberspace, or devise new laws or modes of regulation that can effectively regulate cyberspace. In reaching this result, proponents of this approach argue that localist border theory concepts such as "physical proximity," "locations," and "boundaries" are no longer a prime determinant of the relationship between cause and effect in human interaction online.[133] Acceptance of the so-called "separateness" of cyberspace also encourages an inference that the character of cyberspace law must differ from the character of law governing real space.[134]

Using this new approach, Johnson and Post suggest that we would no longer ask the unanswerable question "where" a Net-based transaction occurred in the geographical world.[135] They argue that the power to control activity in cyberspace has only the most tenuous connections to physical locales.[136] In upholding a typical globalist boundary approach in cyberspace, physical borders no longer function as signposts informing individuals of the obligations assumed by entering into a new, legally significant space.[137] Individuals are unaware of the existence of those borders as they move through virtual space.[138]

Interestingly enough, these two globalist boundary approaches to cyberspace are mostly compared for what they disagree about: whether spatialtiy in cyberspace is separate from that of the physical world. At the same time, it is important to mention that both views also seem to share similar globalist spatial propositions. In fact, both agree that spatiality is mostly a technological concern. By default, both approaches also give only a secondary role to law as a behavioral constraint in cyberspace. Inherently complying with a globalist notion of spatiality, both concur that as much as zoning can serve to uphold on-line locality, strict "gateway" technology zoning is capable of providing a comprehensive boundary theory without the need or ability to construct legal solutions, such as the legal fiction of on-line locales.

As argued below, a preferred localist boundary theory and practice in cyberspace may, in fact, allow us to avoid the technological challenge of zoning cyberspace with totality. To attempt to do so, involves the problematic creation of an inherent continuous

---

TERNET 62 (Brian Kahin & James Keller, eds., 1997); Post, *Governing Cyberspace*, *supra* note 127, at 159.

133 *See, e.g.*, Johnson, *Chaos Prevailing*, *supra* note 127, at 1059.

134 *See* Johnson & Post, *supra* note 114, at 1379, 1381.

135 *Id.*

136 *Id.* at 1371.

137 *Id.* at 1375.

138 *Id.*

space within cyber locales and the erection of outer boundaries surrounding cyberspace. Based on the accumulated experience of law and political geography in application of localist boundary theory, this technocentristic globalist boundary center of attention on outer boundaries and inner continuation is, in fact, of marginal practical importance. It puts less emphasis on both the sufficiency of inner, discontinuous, and differentiated boundaries and locales, and the relative, adaptive, and constructive nature of legal reasoning at large. Additionally, it also falls short of adhering to a legal zoning solution in the case that technology fails, while wrongly concluding that because physical borders are not applicable, the remaining alternative to zoning is technological. As Maureen O'Rourke rightly suggests, notwithstanding the importance of how law will eventually evolve in network environments, such as cyberspace, it is at least as important to fill a gap with legal reasoning by discussing not only the boundaries between and within physical and virtual space, but also the boundaries between different sets of law.[139] Accordingly, there is a need not only for an understanding of what legal rules govern, but also how they relate to each other.[140] In disagreement with these globalist boundary approaches, this study later argues that such legal solutions do not assume perfect scientific solutions, but legally functional and comprehensive ones.

B. *Anti-globalist Boundary Theory: Hunter and Lemley*

Following the globalist approach, lies an antithesis boundary theory. The anti-globalist boundary theory, like the globalist theory, also views the question of on-line spatiality as a question of strictly realistic factual or scientific truth. As a result, we are told that "it is wishful thinking to assume that geographic indeterminacy will prevail and that the Internet is pure information."[141] Accordingly, courts can and should take the differences between cyberspace and the physical world into account[142] because this notion can have a profound consequence for legal analysis.[143] As according to Lemley, "the recognition that the Internet is not just like the physical world, and that the ways in which it is different

---

139 *See* Maureen A. O'Rourke, *Fencing Cyberspace: Drawing Borders in a Virtual World*, 82 MINN. L. REV. 609, 613, 641-45 (1998).

140 *Id.*

141 *See, e.g.*, Joel R. Reidenberg, *Yahoo and Democracy on the Internet*, 42 JURIMETRICS J. 261, 274 (2002).

142 *See* Lemley, *supra* note 97, at 523; O'Rourke, *supra* note 97, at 561.

143 *See* O'Rourke, *supra* note 97, at 592 & n.62 (referring to ROBERT G. SACHS, THE PHYSICS OF TIME REVERSAL 1 (1987)).

may matter to the outcome of cases, is critical."[144] Consequently, strict factual or scientific truth holders, such as Hunter and Lemley, tell us that because cyberspace is not just like the physical world, courts inappropriately use this metaphor. Their main message is that cyberspace is not a real global space, and tangible objects do not exist in locales "there."[145] Thus, rejecting the globalist spatial assumption for cyberspace, they suggest that the analogy between the Internet and a physical space and locales is not sustainable.[146] Nevertheless, these views arguably undermine the importance of the legal constraint in the search for comprehensive and sustainable boundary solutions. According to this version of the boundary discourse, globalist factual or scientific truths stand for a skeptical view of the technological constraint.

Both the globalist and the anti-globalist approaches for cyberspace seem to uphold an absolutist view of the question of on-line spatiality, while adhering to an "all-or-nothing" regulatory analysis regarding the existence of a globalist perception of an on-line space. From a legal perspective, this technocentristic factual or scientific truth should, instead, be only one parameter in establishing a legal truth and should be but the handmaiden for legal reasoning.[147] In opposition to these views, arguably, legal analysis must now expand existing jurisdictional rules into workable legal doctrine in cyberspace through the prism of the localist boundary approach widely adapted to law in the physical world.

II. THE LOCALIST BOUNDARY SYNTHESIS: A LEGAL FICTION OF ON-LINE LOCALES

A. *Overview*

An inclusive legal truth that would formalize on-line spatiality is, in fact, a tentative scientific truth, backed by legal values. The latter could be constructed by courts or other regulatory institutions fictitiously, as in the case of cyber spatiality. Most notably, Lon L. Fuller frames a legal fiction as a false statement recognized as having utility,[148] or a statement propounded with a complete or

---

144 Lemley, *supra* note 97, at 526.

145 *See* Hunter, *supra* note 97, at 472; Lemley, *supra* note 97, at 523; Hardy, *supra* note 97, at 217; O'Rourke, *supra* note 97, at 567.

146 *See* Lemley, *supra* note 97, at 523; Josh A. Goldfoot, *Antitrust Implications of Internet Administration*, 84 VA. L. REV. 909, 920 (1998).

147 *See* John I. Thornton & Joseph L. Peterson, *On Subordination of "Scientific Truth" to "Legal Truth," in* 3 MOD. SCI. EVIDENCE, Part IV. FORENSIC SCIENCES § 24-1.3 (2d ed. 2002). For further explanation, see discussion *infra* Part III.

148 *See* LON L. FULLER, LEGAL FICTIONS 9 (1967).

partial consciousness of its falsity.[149] Part III will show that both settings entail a more pragmatic framework to formalizing on-line locales whenever localist boundary theory is applied.

A legal fiction is constructed through a three criteria classification scheme. First, a legal fiction has to be based on an inference justified by common experience on two levels. It has to be grounded on absence of other proof and be drawn from available evidence. Second, it has to be formalized as either conclusive or freely rebuttable. Finally, a legal fiction has to be phrased in realistic terms. A final construction of a legal fiction of on-line locales based on its meaning in localist boundary theory would then comply with the line of argument suggested herein; this argument asserts that eventually positive law, and particularly territorial privacy, can and should be applied to cyberspace. Whenever the legal fiction of on-line locale can prove useful, cyberspace should not be immune from legal reach.

B. *The Epistemological Framework*

1. Recognition of Utility

A legal fiction can be a false statement recognized as having utility.[150] Such legal fictions would then be constructed upon their functionality.[151] That requirement is also met by localist boundary theory, suggesting that there should be a local center providing a local public or private good commonly provided in network environments. In other words, the periphery should be able to determine a regulative function comprising all aspects of law as a local public or private good which could suit the utility of the legal system at large. For that matter, the construction of on-line locales upon their functionality should be based on three conditions. The first is the preliminary recognition that such distinctive locales are actually necessary. The second is that strict technological solutions would not suffice. The third is that the construction of on-line locales upon their functionality would need to be based on the alternative certainty that formalizing legal locales on-line is feasible.

---

149 *Id.*

150 *Id.* A parallel shift towards a utilitarian approach was also witnessed in boundary theory. After the Second World War, the emphasis in political geography had shifted from the criteria by which a boundary is drawn, to the function which it performs. *See* J.V. Minghi, *Boundary Studies in Political Geography*, in THE STRUCTURE OF POLITICAL GEOGRAPHY: THEORY AND APPLICATIONS 146 (R.E. Kasperson & J.V. Minghi eds., Aldine 1969); *see also* introduction to THE STRUCTURE OF POLITICAL GEOGRAPHY, *supra*, at 77-78.

151 Consequently, after their useful function has ended, legal fictions should and could be readily removed. *See* Aviam Soifer, *Reviewing Legal Fictions*, 20 GA. L. Rev. 871, 875 & n.11.

a. Lack of Distinctive Locales

Arguably, the present inclination to either undermine demarcation between locales on-line in favor of globalist boundary theory support for homogenous continuation (as manifested by Johnson and Post), or reject boundary theory *ab initia*, while implicitly upholding only privately oriented privacy policies (as reaffirmed by other scientific truthists), nevertheless seems to be based on a largely accepted deformation of cyberspace's architecture, in comparison to that of the physical world's. This distortion is largely threefold: the reference to cyberspace's initial private sphere default rule design, the lack of separate transfer costs through neighboring locales, and the low transaction costs of entry into them.

First, historically, it has to do with the opposite way in which the public/private distinction has evolved in the physical world in comparison to cyberspace. In the physical world, the public/private distinction arose out of a double movement in modern political and legal thought.[152] On the one hand, with the emergence of the nation-state and theories of sovereignty in the sixteenth and seventeenth centuries, ideas of distinctly public locales began to take shape.[153] On the other hand, in reaction to the claims of monarchs, and later parliaments, of the unrestrained power to make law, a countervailing effort to stake out distinctively *private* locales free from the encroaching power of the state developed.[154] With the expansion of the latter trend, natural rights theories were elaborated in the seventeenth century for the purpose of setting limits on state power, both over property and religious conscience.[155] In the United States, "[b]y 1934, the areas that people considered the most valuable for mines, agriculture, forestry, water development, and other uses had already been appropriated."[156] What was left behind (to what later became the vastly overextended

---

152 For a thumbnail sketch of the Anglo-American origins of the distinction, see Morton J. Horowitz, *The History of the Public/Private Distinction*, U. PA. L. REV. 1423, 1423 n.1 (1982) (referring to DONALD W. HANSON, FROM KINGDOM TO COMMONWEALTH 1-19 (1970)). For the North American experience, see Gerald E. Frug, *The City as a Legal Concept*, 93 HARV. L. REV. 1059 (1980) (Frug works almost exclusively from secondary sources). *See also* H. HARTOG, PUBLIC PROPERTY AND PRIVATE POWER: THE COOPERATION OF THE CITY OF NEW YORK IN AMERICAN LAW 1730-1870 (1983) (Hartog's book examines New York City from the early eighteenth until the late nineteenth century. His thesis, which he documents in rich detail, is that New York City in the eighteenth century acted as a borough whose charter mixed public and private powers).

153 *See* Horwitz, *supra* note 152, at 1423.

154 *Id.* at 1423 n.3 (referring to historical sources to support that observation).

155 *Id.* at 1423.

156 Carol Rose, *Romans, Roads, and Romantic Creators: Traditions of Public Property in the Information Age*, 66 LAW & CONTEMP. PROBS. 89 (referring to GEORGE CAMERON COGGINS ET AL., FEDERAL PUBLIC LAND AND RESOURCES LAW 133-34 (4th ed. 2001)).

Bureau of Land Management) were those lands that the settlers considered worthless, or at least more trouble than they were worth—*res nullius*, it seemed, and likely to stay that way.[157] During the early years of the conservative Burger Court, the private sphere was narrowed further.[158] Thus far, in the physical world, an interventionist theory to limit the private sphere has not prevailed, and the public sphere continues to serve as the default rule.[159] Instead, courts have identified constitutional law with the task of defining and expanding private spheres within which individuals must be left free from the default public domain ruled by governments.[160]

In cyberspace, the opposing trend unmistakably has prevailed. While the physical world is presently subject to a default rule of a continuous public sphere that is then subject to distinct proprietary private sphere allotments, cyberspace architecture imbeds a different structure. In the latter, apart from the Internet's "public roads" or backbone transit infrastructure, which is regulated according to telecommunications and antitrust law, the present default rule contains a mosaic of private allotments, namely, neighboring proprietary websites. As pictorially put by Maureen Ryan, cyberspace has "no town halls, no granges, no public squares, no downtown churches or galleries or schools."[161] Thus, neither public locales nor balanced territorial privacy policy have been established. Instead, only a private privacy legal rule has been adopted—and too widely so. Cyberspace's architecture, backed by the "hands off" paradigm towards privacy policy at large, has led to this deformation. In the present post-industrial society,[162] where information such as the Internet's is a major source of

---

157 COGGINS, *supra* note 156, at 133-34, 139, 142-43.

158 *See, e.g.*, Donald R.C. Pongrace, *Stereotypication of the Fourth Amendment's Public/Private Distinction: An Opportunity for Clarity*, 34 AM. U. L. REV. 1191, 1191-92 & nn.6-8 and accompanying text (describing a process of narrowing the private sphere during the 1980's, in the years of the Burger Court). Commentators use the term "Burger Court" to signify the conservative majority that currently dominates the United States Supreme Court. *See* Herman Schwartz, *Fifteen Years of the Burger Court*, THE NATION, Sept. 24, 1984, at 262 (describing the Court's conservative trend since Warren Burger started his first term as Chief Justice in 1969).

159 *See* Louis Michael Seidman, *Public Principle and Private Choice: The Uneasy Case for a Boundary Maintenance Theory of Constitutional Law*, 96 YALE L.J. 1006, 1011 & n.17 and accompanying text (1986) (adding that there always existed an alternative tradition in American constitutional law of preventing private corporations from interfering with freedom of speech). For a discussion of the confusion that is generated when the two traditions clash, see G. STONE ET AL., CONSTITUTIONAL LAW 575-78, 739-41 (1986).

160 *See* Seidman, *supra* note 159, 1010-11 & n.18 and accompanying text.

161 Maureen Ryan, *Cyberspace as a Public Space: A Public Trust Paradigm for Copyright in a Digital World*, 79 OR. L. REV. 647 & n.249 and accompanying text (2000).

162 On the shift from the industry economy to the present information economy, see

wealth aggregation, what has been the original exception seems to have become the norm.[163] As Carol Rose points out, this "propertization" trend did not occur in a vacuum, but rather came directly at the expense of what might seem to be "un-ownable" diffuse resources or *res communes* in the tangible world.[164] Left to self-regulatory approaches, sufficient and legally protected public locales arguably will not evolve, and more particularly, an inner balance between private and public locales and territorial privacy policy, will not be achieved.[165]

Second, as opposed to the physical world, with little scarcity constraint on on-line access and use, would-be entrants to private on-line properties do not objectively value entry more than the landowner would objectively suffer from the entry for transfer purposes and use. In the physical world, where such a reality exists, that means the need to both create public roads and subsidize transfer through neighboring lots. Primarily, this led to the development of the distinction between public and private because private owners needed open access. As a result, access to private locales without consent, and the creation of a limited privilege to trespass, was rarely done voluntarily, as explained. Moreover, conditions such as emergency or physical distance often made it unusually difficult for the landowner and would-be entrant to bargain on the conditions for entry.[166] The reason is manifest: entrants may damage crops, commit thefts, and do other mischief. That is why open access was then added as a public rule. However, in cyberspace there is no need for access permission through private allotments, and, thus, no additional need for particular public locales *between* them has emerged. Instead, transfer between private allotments is primarily done through ex-jurisdictional public roads in the form of cyberspace's backbone transit services. Gateway homepages, the entrance to private websites, are not dependently accessible among themselves and for that reason were not seen as inflicting additional transfer costs to neighboring private locales. In summary, in cyberspace, there is no need for transfer permission between private websites. Neither is there an inherent techni-

---

Mell, *supra* note 93, at 17 (referring to DANIEL BELL, THE COMING OF THE POST-INDUSTRIAL SOCIETY 47-119 (1973)).

163 Lessig, *The Architecture of* Privacy, *supra* note 120, at 60.

164 *See* Rose, *supra* note 156, at 94; *see also* Paolo Carpignano et al., *Chatter in the Age of Electronic Reproduction: Talk Television and the "Public Mind," in* THE PHANTOM PUBLIC SPHERE 93, 96-97 (Bruce Robbins ed., 1993) (relating this pattern to the more broad influence of mass media).

165 For further enlightenment, see discussion *infra* Part III.C.2.

166 Robert C. Ellickson, *Property in Land*, 102 YALE L.J. 1315, 1383-84 (1993).

cal need to subsidize transfer costs through the construction of public locales as a means of economizing on additional transfer costs.

Moreover, transfer costs are also lower in cyberspace whenever the transferee's destination is a would-be public locale. In some cases, forum providers *voluntarily* set aside some area for open use within private websites (or would-be private locales), thus diminishing the need to transfer between separate locales. Major Internet providers are obvious candidates for the modern application of this principle, as they use their message boards and chat rooms to foster a sense of community. Sites, such as eBay and Amazon.com, whose purpose is strictly private e-commerce, confirm this observation. This is also the prevailing practice in real time "chat rooms,"[167] news groups,[168] and remote information retrieval practices such as bulletin-board services and message boards.[169] Notwithstanding the significance of these new developments in cyberspace's boundary equilibrium, neither the present architecture of cyberspace, nor the present day United States federal government's technocentristic self-regulation approaches, enhance these areas to the protected legal status of public locales. They also do not reestablish the balance between both types of locales but rather favor the latter. Third, as opposed to the physical world, transaction costs generated by website landowners and would-be entrants to negotiate a license or easement of entry for open public use, without the use of any licensing regimes, are relatively low. As a result, with no need for the corrective minimization of transaction costs, preservation of the present private allotment mosaic seems to remain stable, while socially implying inefficient allocative results.

b. The Insufficiency of Technological Solutions

The lack of inner equilibrium between the different types of locales ultimately may have enticed policy makers and theoreticians alike to make the normative leap: law suffers from an inher-

---

167 Chat rooms allow interested individuals to participate in on-line discussions in real time on myriad general interest topics by sending and receiving messages via their ISP. *See generally* ACLU v. Reno, 929 F. Supp. 824, 834-36 (E.D. Pa. 1996) (surveying common methods of communication on the Internet).

168 Usenet newsgroups are a loosely organized collection of distributed bulletin boards, each one dedicated to a particular topic. *See id.* (surveying common methods of communication on the Internet); *see also* Loving v. Boren, 956 F. Supp. 953, 954 (W.D. Okla. 1997), *aff'd*, 133 F.3d 771 (10th Cir. 1998) ("News groups are interactive 'places' on the Internet.").

169 *See generally*, ACLU v. Reno, 929 F. Supp. at 834-36.

ent inability to correct this anomaly. That is, as the analogy between the Internet and a physical locale is not particularly strong,[170] scientific truism largely upholds that it is wishful thinking to assume that legally made geographic indeterminacy could prevail.[171] The recognition that the Internet is not just like the physical world, and that the ways in which it is different may matter to the outcome of cases, we are told, is critical.[172] In fact, the United States federal government's privacy policy still encourages the withdrawal of law as a balancing constraint. The FTC's stance toward online privacy, which emphasizes self-regulation via the adoption of privacy policies, is an example of this.[173] However, technology alone has failed to provide protection comparable to that which is provided in law.[174] Technology as a regulatory constraint, at least presently, is incapable of establishing a comprehensive boundary solution by itself for three main reasons: its inherent inability to self-provide with a public/private distinction, its poorly practiced appeal, and its lack of compliance with existing law.

To begin with, as a technological solution, "gateway" or access-based zoning is essentially used to restrict only private locales ex-ante, namely proprietary websites. In addition, demarcation lines among network service providers such as America Online, CompuServe, or Prodigy only generate important boundaries around privately owned proprietary services. Private contractual arrangements determine the availability and the conditions of access for network connections.[175] Without a gateway, interactions are effectively prohibited.[176] Thus, technology does not support an inherent distinction between public and private locales, but rather only

---

170 *See, e.g.*, Lemley, *supra* note 97, at 523; Goldfoot, *supra* note 146, at 920 ("At best 'cyberspace' is a convenient term describing a set of communications achieved through the Internet.").

171 *See, e.g.*, Reidenberg, *supra* note 141, at 274; Resnick, *supra* note 126, at 396; Lessig, *The Death of Cyberspace*, *supra* note 126, at 344; Johnson & Post, *supra* note 114, at 1379; Johnson, *Chaos Prevailing*, *supra* note 127, at 1059; Post, *Governing Cyberspace*, *supra* note 127, at 161.

172 *See* O'Rourke, *supra* note 97, at 592 & n.62. (referring to SACHS, *supra* note 143, at 1).

173 *See* Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041 (2000); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 508-11 (1995).

174 *See* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, STAN. TECH. L. REV. 1, 79 (2001); Joel R. Reidenberg et al., Symposium, *Data Privacy Laws and the First Amendment: A Conflict? Panel II: The Conflict Between Commercial Speech and Legislation Governing the Commercialization of Private Sector Data*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 59, 60 (2000); Reidenberg, *supra* note 27, at 771.

175 *See* Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 Emory L.J. 911, 917 (1996).

176 *Id.* at 918.

the further fencing of private locales, ultimately taking no notice of the needed public ones.

Second, even for private locales, this solution is poorly practiced because it decreases the level of accessibility and attractiveness of websites that choose to independently construct fences around themselves. As a result, as some courts have already recognized, although gateway technology has been available on the World Wide Web for some time, it is not available to all web users,[177] and it is just now becoming technologically feasible for chat rooms and USENET newsgroups.[178] Gateway technology is not omnipresent in cyberspace, and because without it there is no means of age verification, cyberspace still remains largely unzoned—and unzoneable.[179] As courts have recognized, for user-based zoning to be effectual, an agreed-upon code (or "tag") would have to be present. Then, screening software or browsers with screening capabilities would have to be able to identify the "tag." Those programs would have to be extensively available, and widely used by Internet users. Presently, none of these circumstances prevail.[180] It is still the case that screening software "is not in wide use today" and "only a handful of browsers have screening capabilities."[181] Furthermore, there is no agreed-upon "tag" for those programs to identify.[182] As a substitute, such "gateway" technology still requires Internet users to enter identifiable information about themselves before they can access the countless private locales of cyberspace.[183]

Third, strict technologically-based zoning is not backed by the protective measurements of the Digital Millennium Copyright Act ("DMCA"). Thus, such zoning does not seem to invalidate the requirement for a contractual framework in case territorial privacy is ignored.[184] Since the enactment of the DMCA in 1998, the Copyright Act has addressed access to copyrighted material as well as the scope of exclusive rights therein.[185] Under the DMCA, it is illegal to "circumvent a technological measure that effectively controls ac-

---

177 *See* Reno v. ACLU, 521 U.S. 844, 845 (1997); Shea v. Reno, 930 F. Supp. 916, 933-34 (S.D.N.Y. 1996).

178 *See Reno v. ACLU*, 521 U.S. at 891.

179 *See* ACLU v. Reno, 929 F. Supp. 824, 845-46 (E.D. Pa. 1996); *Shea*, 930 F. Supp. at 934.

180 *See Shea*, 930 F. Supp. at 945-46.

181 *Id.*

182 *See ACLU v. Reno*, 929 F. Supp. at 847-48; *Shea*, 930 F. Supp. at 945.

183 *See ACLU v. Reno*, 929 F. Supp. at 845.

184 For the alternative solution based on territorial privacy, see discussion *infra* Part III.C.2.a.

185 *See* 17 U.S.C. § 1201 (Supp. IV 1998).

cess to a work protected" by copyright.[186] But only those access control measures that "require the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work," are protected against circumvention.[187] Most e-commerce websites, such as eBay, contain some copyrighted material in addition to their uncopyrighted product and pricing information. However, they do not use access control measures protected by the DMCA, in part because such steps would discourage entry by welcome, as well as unwanted, visitors.[188] As a result, technological zoning assumes a contractual relationship, whereas due to the lack of sufficient will and implementation of identification and contractual consent, such a solution is still inefficient. A territorially-based solution that would only necessitate unilateral notice at the entrance to on-line locales should be preferred because it may overcome the need for identification and contractual consent.[189] As a practical matter, observance in private locales should be replaced through a mechanism of voluntary disclosure of whichever types of information, namely transactional, registration, and clickstream data, that would be abided to by would-be entrants.[190] However, in public locales, observance of the website's accumulated data files should be freely allowed, as long as a notice of the public locale is clear and conspicuous. However, public locales then should be solely restricted to the collection of non-identifiable registration and clickstream data.[191]

Law, if constructed to be, can easily overcome any of these geographical discontinuities that such digital coercion threatens to entail. Continuity in the spatial pattern of preferences should then suggest a need to define peripheral locations in a more narrow and gradual form, implying that such a boundary would be valuable.[192] Thus, a localist boundary theory would put emphasis on drawing boundaries that should evolve through a case-by-case common law development in which tribunals seek guidance in legislation and treaties. Various courts already uphold the value of this regulative approach for trespass analysis in cyberspace.[193] In the physical

---

186 *Id.* at § 1201(a)(1)(A).

187 *Id.* at § 1201(a)(3)(B).

188 *See* O'Rourke, *supra* note 97, at 583-84 & n.95 and accompanying text.

189 For further analysis, see discussion *infra* Part III.C.2.a.

190 *See* Richard B. Parker, *A Definition of Privacy*, 27 RUTGERS L. REV. 275, 280 (1974); *see also* Gavison, *supra* note 1, at 432-33.

191 *See* Parker, *supra* note 190, at 280; *see also* Gavison, *supra* note 1, at 432-33.

192 *See* Stone, *supra* note 98.

193 *See* Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 473-4 & n.6 (Ct. App. 1996) (concluding that electronic signals generated by computers that minors used to access plaintiff's telephone system were sufficiently tangible to maintain action for trespass to

world, this sort of dialogue between courts and lawmakers in delineating the geographic limits is the heart of what Farber calls, in the context of international environmental law, the evolutionary approach.[194] In the midst of a technological regulatory vacuum, and due to the arguable sufficiency of the legal solution, this same approach should ultimatey hold for cyberspace.

c. The Sufficiency of Legal Solutions

A functional existence of such a distinction between a public and private sphere or locale of human activity, primarily, is a central tenet of jurisprudence in liberal democracy.[195] The appearance of capitalist market relations as a self-regulating economic system has enhanced the centrality of private individualism that was then fenced against public intrusions. Overall, in Western democracies, it was market growth that shaped political and legal interactions between both spheres.[196] Notably, in the present service economy, information has become an increasingly valuable commodity.[197] That development also eventually penetrated the various legal fields and became impossible to ignore.[198] Notably, as a

---

personal property, and commenting on applying common law to modern facts); *see also* CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (relying on *Thrifty-Tel* for support in finding electronic signals sufficient for trespass to chattels action).

194 *See* Farber, *supra* note 98, at 1273; Stone, *supra* note 98.

195 For examples of U.S. federal court decisions upholding the difference between public sphere and private sphere, see United States v. Knotts, 460 U.S. 276, 284 (1983) (citing United States v. Knotts, 662 F.2d 515, 518 (8th Cir. 1981)), which discusses human activity in terms of public and private spheres, and United States v. Bailey, 628 F.2d 938, 941-43 (6th Cir. 1980) which notes the distinction between activity in public and private spheres. *See also* Robert H. Mnookin, *The Public/Private Dichotomy: Political Disagreement and Academic Repudiation*, 130 U. PA. L. REV. 1429 (1982) (noting distinction between public and private spheres relating to individual rights vis-à-vis government powers).

196 *See* TRENT SCHROYER, THE CRITIQUE OF DOMINATION (George Braziller ed., 1973); JÜRGEN HABERMAS, LEGITIMATION CRISIS (Thomas McCarthy trans., Beacon Press 1975); Andrew Fraser, *The Legal Theory We Need Now*, 1978 SOCIALIST REV. 147 (1978); Ellen Wood & Ellen Meiksins, *The Separation of the Economic and the Political in Capitalism*, 127 NEW LEFT REV. 66 (1981).

197 *See* Mell, *supra* note 93, at 26-41 (stating that information has always been a core resource, referring to Anthony G. Oettinger, *Information Resources: Knowledge and Power in the 21st Century*, 209 SCIENCE 191 (1980)).

198 For different legal applications regarding the distinction, see, for example, Karl E. Klare, *The Public/Private Distinction in Labor Law*, 130 U. PA. L. REV. 1358 (1982) (showing how the public/private distinction is used in historical studies of legal change). *See* Isaac Balbus, *Commodity Form and Legal Form: An Essay on the Relative Autonomy of the Law*, 11 LAW & SOC'Y REV. 571 (1977) (for a social science approach to the relationship between political economy and the public/private distinction in law). For a critical view of this movement, see Duncan Kennedy, *The Stages of Decline of the Public/Private Distinction*, 130 U. PA. L. REV. 1349 (1982), for an internal critique of the public/private dichotomy in legal discourse. Any progress with this paper's claims would first confront Duncan Kennedy's notable critique of the public/private initial dichotomy. In retrospect, Kennedy's claim remained a cry in the wilderness. As Ellickson concludes, all analysts now agree that it is important to uphold the private/public distinction. *See* Ellickson, *supra* note 166, at 1381.

legal concern, the private/public distinction also came to be known for its application on questions of legal jurisdiction, examining the mechanisms by which legal boundaries could be established and altered.[199]

In a seminal study on the public sphere, Carol Rose indicates that in the American legal tradition there were largely three types of theories to justify public locales, as exemplified by waterfront beach cases.[200] The first theory is "custom," where the public asserts ownership of property under some claim so ancient that it antedates any memory to the contrary.[201] Clearly, network environments such as the Internet are far too young to give rise to such ancient claims that antedate any memory to the contrary. Nevertheless, there is no inherent reason to assume that such a claim could not evolve in cyberspace in the long-run. The second theory is a "prescriptive or dedicatory" theory, where a period of public usage gives rise to an implied grant or gift from private owners.[202]

Moreover, even Kennedy himself has reconsidered this approach. *See* Peter Gabel & Duncan Kennedy, *Roll Over Beethoven*, 56 STAN. L. REV. 1, 15 (1984).

Nevertheless, in response to Kennedy's critique, two central observations could be made. First, based on his normatively-neutral two-stage test, Kennedy upholds that he never inherently denies the distinction's normative potential to survive the test. Instead, Kennedy's argument suggests that such a distinction is no longer practical in the current legal system, and should thus not prevail. This is based on the view that the range of distinctions that characterize liberal legality, "state/society, individual/group, right/power, contract/tort, law/policy, legislative/judiciary, objective/subjective, reason/fiat, freedom/coercion" are all going through "similar processes of decline." Kennedy, *supra*, at 1349-50. At least on this factual ground, Kennedy's argument might seem to be too adventurous. *See, e.g.*, Seidman, *supra* note 159, at 1006 (arguing that during the Lochner era an assumption of "natural" boundary was made in the Supreme Court); *see also* Lochner v. New York, 198 U.S. 45 (1905). For a supporting survey of the era, see STONE, *supra* note 159, at 739-41.

Second, Kennedy is inherently unconcerned with the exact substance of each sphere, but he assumes their practical existence. *See* Kennedy, *supra*, at 1350. Thus, in his somewhat tautologous structure, separate spheres, such as individual/group, right/power, contract/tort, may, nevertheless, exist as long as no boundary is put in place between them. Arguably, once separation in content between spheres exists, albeit even vague or otherwise unclear, any justification in ignoring the boundary in between should only be possible in marginal, extreme situations. *See* discussion *infra* Part III.B.1.

199 *See, e.g.*, Jeff Weintraub, *The Theory and Politics of the Public/Private Distinction*, *in* PUBLIC AND PRIVATE IN THOUGHT AND PRACTICE: PERSPECTIVES ON A GRAND DICHOTOMY 9 (Jeff Weintraub & Krishan Kumar eds., 1997); Frug, *supra* note 152, at 1059.

200 *See* Berger, *supra* note 93, at 655-59.

201 Carol Rose, *The Comedy of the Commons: Custom, Commerce, and Inherently Public*, 53 U. CHI. L. Rev. 711, 714 & n.16 (referring to courts in Florida, Hawaii, and Oregon that have adopted this approach: City of Daytona Beach v. Tona-Rama, Inc., 294 So. 2d 73 (Fla. 1973); County of Hawaii v. Sotomura, 517 P.2d 57 (Haw. 1973); *In re* Ashford, 440 P.2d 76 (Haw. 1968); Thornton v. Hay, 462 P.2d 671 (Or. 1969)).

202 *See* Rose, *supra* note 201, at 714 & n.15 (referring to Gion v. City of Santa Cruz, 465 P.2d 50 (Cal. 1970)). Other states in which courts have recently applied the 'implied dedication' or prescriptive approach to the waterfront are Texas, in Seaway Co., Inc. v. Attorney General of Texas, 375 S.W.2d 923 (Tex. 1964), and—somewhat reluctantly—New York, in Gewirtz v. City of Long Beach, 330 N.Y.S.2d 495 (Sup. Ct. 1972), *aff'd*, 358 N.Y.S.2d 957 (App. Div. 1974) (mem.); *cf.* Dep't of Natural Res. v. Mayor of Ocean City, 332 A.2d 630

In cyberspace, such a theory might be too limited in scope to undermine the ability and incentives of website owners to explicitly limit privacy protection by giving notice of a public sphere. The third is a "public trust" theory, where the public always has rights of access to the property in question, and any private rights are subordinate to the public's "trust" rights.[203] Carol Rose calls such lands "inherently public property."[204] In the physical world, the American legal system has strongly suggested that some kinds of property should not be held exclusively in private hands, but should be open to the public, or at least subject to what Roman law called the *jus publicum*, or the "public right."[205] Under the "inherently public property" (*jus publicum*) doctrine, for the public to claim property, two elements were essential: first, either the property had to be capable of monopolization by private persons, or was without protections securing public access against such threats;[206] second, the public's claim had to be superior to that of the private owner because the property was most valuable when used by an indefinite and unlimited number of people, or by the public at large.[207] Courts have become receptive to requests to extend this theory to preserve a public sphere beyond its traditional water-related focus. The public trust doctrine has been invoked to support claims for the preservation of many types of property deemed public resources, including parks,[208] marshlands,[209] and archeological

---

(Md. 1975) (doctrine held inapplicable because no clear intent to dedicate); State v. Beach Co., 248 S.E.2d 115 (S.C. 1978) (no intent to dedicate). For commentary, see Margit Livingston, *Public Access to Virginia's Tidelands: A Framework for Analysis of Implied Dedications and Public Prescriptive Rights*, 24 WM. & MARY L. REV. 669 (1983); Michael A. O'Flaherty, Note, *This Land Is My Land: The Doctrine of Implied Dedication and Its Application to California Beaches*, 44 S. CAL. L. REV. 1092 (1971).

203 *See* Rose, *supra* note 201, at 714 & n.14 (referring to State v. Superior Court, 625 P.2d 239 (Cal. 1981)); *see also* City of Berkeley v. Superior Court, 606 P.2d 362 (Cal. 1980); Van Ness v. Borough of Deal, 393 A.2d 571 (N.J. 1978); Borough of Neptune City v. Borough of Avon-by-the-Sea, 294 A.2d 47 (N.J. 1972); Matthews v. Bay Head Improvement Ass'n, 471 A.2d 355 (N.J. 1984); Just v. Marinette Country, 201 N.W.2d 761, 768-69 (Wis. 1972).

For physical world context, see Note, *The Public Trust in Tidal Areas: A Sometime Submerged Traditional Doctrine*, 79 YALE L.J. 762 (1970). *See* Robert T. Burke, Comment, *Public or Private Ownership of Beaches: An Alternative to Implied Dedication*, 18 UCLA L. REV. 795 (1971); Jonathan M. Hoff, Note, *Public Beach Access Exactions: Extending the Public Trust Doctrine to Vindicate Public Rights*, 28 UCLA L. REV. 1049, 1069-86 (1981). For cyberspace context, see Maureen Ryan, *supra* note 161, and Molly S. van Houweling, *Cultivating Open Information Platforms: A Land Trust Model*, 1 J. TELECOMM. & HIGH TECH. L. 309 (2002).

204 Rose, *supra* note 201, at 720.

205 *See id.* at 715-16 & n.10 and accompanying text (referring to Scheiber, *Public Rights and the Rule of Law in American Legal History*, 72 CAL. L. REV. 217 (1984)); *see also* Molly Selvin, *The Public Trust Doctrine in American Law and Economic Policy, 1789-1920*, 1980 WIS. L. REV. 1403. For the *jus publicum* (or *publici juris*) language, see Commonwealth v. Alger, 61 Mass. (7 Cush.) 53, 76 (1851) (discussed in Scheiber, *supra*, at 222).

206 Rose, *supra* note 201, at 774.

207 *Id.*

208 *See, e.g.*, Paepcke v. Public Bldg. Comm'n, 263 N.E.2d 11 (Ill. 1970); Wade v. Kramer,

sites.[210] Accordingly, courts have repeatedly found public places to be ex-jurisdictional locations for private excludability.

In the digital era, without acknowledging a separate public sphere, there is no "place" left for unilateral, non-identifiable data collection for either non-commercial or commercial purposes alike. Policymaking should now further legitimize the expansion of information collection in public locales in cyberspace. The only way to balance that activity with private territorial privacy protection policies, as it is balanced in the physical world, would be to uphold distinctive public and private locales. In that regard, the claim that certain portions of cyberspace deserve, or would require, a public on-line locale status should become compelling.[211]

2. Consciousness of Falsity

Words or phrases that take on a legal function, such as "non-material locales," are propounded with a recognition of their utility, while a legal fiction arises with complete or partial consciousness of its falsity. In the Anglo-American jurisprudence, it is widely acknowledged that no court should base a decision solely on cognitive science if doing so would exclude the different values of the law, such as fairness and justice to the litigants.[212] Arguably, this should also enhance the experience of formalizing a localist boundary theory for cyberspace based on a legal fiction of locales.

There are two distinctions that narrow the subject matter of any legal fiction. The first is the distinction between a fiction and a lie.[213] A fiction is distinguished from a lie by the fact that it is not meant to deceive.[214] The user of a legal fiction does not intend to produce belief in those who hear or read it. Neither should a user of a legal fiction believe the false statement. It is probably the case that, thus far, no such intentional lie was introduced into the

---

459 N.E.2d 1025 (Ill. App. Ct. 1984); Gould v. Greylock Reservation Comm'n, 215 N.E.2d 114 (Mass. 1966).

209 *See, e.g.*, Freeborn v. Bryson, 210 N.W.2d 290 (Minn. 1973).

210 *See, e.g.*, San Diego County Archaeological Soc'y v. Compadres, 146 Cal. Rptr. 786 (Cal. 1978) (holding that the public trust doctrine cannot be extended to cover archeological remains located on private property).

211 *See* Goldstone, *supra* note 96, at 3.

212 *See, e.g.*, Akron, Canton & Youngstown Railway Company v. United States, 261 U.S. 184, 197 (1923) ("*New England Divisions Case*"); R.R. Comm'n of Wisconsin v. Chicago, Burlington & Quincy R.R. Co., 257 U.S. 563, 579 (1922); *see also* Howard T. Markey, *Jurisprudence or "Juriscience?,"* 25 WM. & MARY L. REV. 525, 525-26 (1984).

213 *See* FULLER, *supra* note 148, at 7; *see also* Fed. Power Comm'n v. Fla. Power & Light Co., 404 U.S. 453, 459 (1972), *rev'd and remanded, petition for rehearing denied*, 405 U.S. 948 (1972) (rejecting a jurisprudential approach that meets the standard at law, but it is technologically unsound). For further explanation and analysis, see discussion *supra* Part II.C.1.b.

214 *See* FULLER, *supra* note 148, at 7.

boundary theory discourse regarding on-line spatiality. Therefore, this renders this distinction less relevant to the present analysis. The second and more relevant distinction to the cyberspace spatiality discussion is the distinction between a fiction and an erroneous conclusion.[215] A fiction is generally distinguished from an erroneous conclusion or scientific hypothesis by the fact that its author adopts it with knowledge of its falsity.[216] The author of the legal fiction "either positively disbelieves it or is partially conscious of its untruth or inadequacy."[217] Along these lines, scientific truism has given rise to many commentators who criticize the courts for applying the doctrine of trespass to chattel—especially to cyberspace.[218] Evidently, no statement describing either the physical world or network environments can adequately describe reality. However, Fuller reserved the label of "false," for only those statements that are outstanding or unusual in their inadequacy.[219] Once the label of "false" has attached, and the statement has not been made with intent to deceive, we have a legal fiction.[220] Accordingly, a statement must be false before it can be classified as a fiction.

This perception of truth is relative and pragmatic. The legal truth of any statement is merely a question of its adequacy—whether it comes close to describing reality. Finally, based upon the user's recognition of the statement's falsity, a distinction between a "benign" and "dangerous" legal fiction becomes useful. The "danger" of a legal fiction varies inversely with the acuteness of the awareness that the assumption is false. In other words, a legal fiction is "wholly safe" only when the statement is used with "complete consciousness of its falsity."[221] Fuller considered such a legal fiction benign.[222] On the other hand, a legal fiction becomes "dangerous" only if the user is unaware of the falsity of the statement. One way to avoid this "danger" is for the user of the legal fiction to embellish it with a grammatical motif of its falsity, such as to propose that locales do not technically exist on-line or, instead, to say that their existences are legally fictional. The latter approach could then be justified because technology in cyberspace is not ca-

---

215 *Id.*
216 *Id.*
217 *Id.* at 8.
218 *See* Hunter, *supra* note 97; O'Rourke, *supra* note 97, at 595-97; Dan Burk, *The Trouble With Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 34 (2000).
219 *See* FULLER, *supra* note 148, at 11-12.
220 *Id.*
221 *Id.* at 10.
222 *Id.*

pable of, nor not technically mature enough for, upholding on-line spatiality or self-regulated differentiated locales in their strict scientific sense.[223]

Even if a legal fiction of on-line locales is finally agreed upon, it might still technically be incapable of defining exact jurisdictional boundaries between different locales. As acknowledged for the present proprietary-based information privacy analysis in cyberspace, the idea that an individual has a protected right to control the use of personal information directly conflicts with the concept of the public distribution of information.[224] Yet, as important as it is for a legal system to make an effort to locate this exact jurisdictional boundary—whether or not finding that exact location is possible and should be a finite goal—it is yet more pressing and important for a liberal democratic society to agree on the existence of such a distinction in the first place.[225] Thus, even the ambiguity regarding the appropriate *location* of a boundary between locales is not a unique concern to the digital era.[226] Occasionally, even before the information age, this has been a source of controversy.[227] Since the beginning of the realist movement in American jurisprudence in the 1930's,[228] the boundary's ambiguity has become increasingly obvious.[229] In dealing with this issue, it should be clear at the outset that the system will never operate as cleanly as the rules governing property rights on land.[230] As Richard Epstein describes, for land disputes, it is generally clear when one person has crossed the boundary that separates his or her property from another.[231] The definition and identification of appropriate boundaries is never as clear in disputes over privacy.[232]

This legal intricacy only enhanced the tension that existed in earlier telecommunications systems.[233] One especially notable ex-

---

223 On the institutional explanation for this argument,see discussion *supra* Part III.C.2.

224 *See, e.g.*, NIMMER, *supra* note 1, ¶ 8.05.

225 *See, e.g.*, Solove, *supra* note 10, at 1132.

226 *See, e.g.*, Mell, *supra* note 93, at 4, 22.

227 *See* Mnookin, *supra* note 195, at 1430-34 (discussing various definitions of the dividing line between public and private spheres).

228 For a general description of the realist challenge to formalism that began in the 1920's, see Elizabeth Mensch, *The History of Mainstream Legal* Thought, *in* THE POLITICS OF LAW: A PROGRESSIVE CRITIQUE 26-29 (D. Kairys ed., 1982).

229 For discussions of the current ambiguity surrounding the public/private distinction, see *Papers from the University of Pennsylvania Law Review on the Public/Private Distinction*, 130 U. PA. L. REV. 1289 (1982); Kennedy, *supra* note 198, at 1349.

230 *See* RICHARD A. EPSTEIN, *Deconstructing Privacy: And Putting it Back Together Again, in* The RIGHT TO PRIVACY 7 (Ellen Frankel Paul et al. eds., 2000).

231 *Id.*

232 *Id.*

233 *See, e.g.*, Daniel Bell, *Communications Technology—For Better or for Worse*, HARV. BUS. REV., May-June 1979, at 20, 21.

ample is the merger between telephones and televisions with computers; this resulted in the development of a flexible and diverse international information-exchange system that now allows for the nearly instantaneous transfer of information through cables, satellites, microwave relays, and fiber optics.[234] Nevertheless, simply by maintaining a positivistic right to privacy, both initially upheld the constituting framework of jurisdictional boundaries and thus the need for an inner balance between private and public rationales.[235] Thereby, even accepting these certainty limitations, it is possible to make some measurable progress to a sensible end.[236] Instead of offering reconciliation, constitutional law allows us to live with contradiction by establishing a shifting, uncertain, and contested boundary between distinct public and private locales within which conflicting values can be separately nurtured.[237] Therefore, the legal fiction of on-line locales can, thus, still be seen as *benign*, that is assuming that it is still stated in complete consciousness of its falsity.

Conceptually, the incorporation of a new legal fiction to cyberspace's boundary theory should be seen as a general legal standard. The use of fictions or presumptions is very popular in American jurisprudence and should therefore not be considered extraneous or passé by cyber lawyers.[238] Presumptions, and the associated burdens of proof necessary to overcome them, appear virtually everywhere in law.[239] For example, in property law, a specific legal fiction is the presumption that one who owns soil, owns all

---

234 *Id.*

235 For the view suggesting that the private/public distinction involves especially questions of jurisdiction, see, for example, WEINTRAUB, *supra* note 199, at 9.

236 *See* Epstein, *supra* note 230, at 7.

237 *See* Seidman, *supra* note 159, at 1007.

238 For the leading scholarship on legal fictions, see GUIDO CALABRESI, IDEALS, BELIEFS, ATTITUDES, AND THE LAW: PRIVATE LAW PERSPECTIVES ON A PUBLIC LAW PROBLEM (1985); GUIDO CALABRESI, A COMMON LAW FOR THE AGE OF STATUTES 172-77 (1982); Kathryn Abrams, *A Constitutional Law for the Age of Anxiety*, 73 CAL. L. REV. 1643 (1985) (reviewing CALABRESI, IDEALS, BELIEFS, ATTITUDES, AND THE LAW: PRIVATE LAW PERSPECTIVES ON A PUBLIC LAW PROBLEM (1985)); Block, *Suits Against Government Officials and the Sovereign Immunity Doctrine*, 59 HARV. L. REV. 1060 (1946); James B Stocking, Note, *Penumbras and Privacy: A Study of the Use of Fictions in Constitutional Decision-Making*, 87 W. VA. L. REV. 859 (1985); Ronald J. Allen, *Burdens of Proof, Uncertainty, and Ambiguity in Modern Legal Discourse*, 17 HARV. J.L. & PUB. POL'Y 627 (1994).

However, for some reason, interest cooled down until the 1920's when Roscoe Pound, John Chipman Gray, and Lon Fuller reawakened this dormant jurisprudential technique. *See* Louise Harmon, *Falling Off the Vine: Legal Fictions and the Doctrine of Substituted Judgment*, 100 YALE L. J. 1, 11 (1990).

239 See ROSCOE POUND, INTERPRETATIONS OF LEGAL HISTORY 131 (1923); FULLER, *supra* note 148, at 1; J. Harvie Wilkinson, III, *Toward a Jurisprudence of Presumptions*, 67 N.Y.U. L. REV. 907 (1992); Soifer, *supra* note 151, at 872-75; Antonio E. Bernardo & Ivo Welch, *A Theory of Legal Presumption*, 16 J. L. ECON. & ORG. 1, 2 (April 2000).

the way to the heavens and to the depths.[240] In employment discrimination litigation under Title VII of the 1964 Civil Rights Act, the burden of evidentiary production (and thus the applicable presumption) can shift to the defendant if the plaintiff is a qualified (but rejected) applicant and a member of a historically oppressed group.[241] In constitutional law, the equal protection doctrine implicitly operates as a presumption, requiring a court to determine a "level of scrutiny" to apply to a challenged statutory or regulatory classification.[242] In corporate law, a separate legal personality has been fictitiously constructed for corporations.[243] A legal fiction is commonly seen as an assumption which conceals, or attempts to conceal, the fact that a rule of law, such as differentiated private and public on-line locales in cyberspace, has undergone alteration, yet its letter remained unchanged.[244] Thus, the fiction of "inviting" in the "attractive nuisance" cases is intended to escape the rule that there is no duty of care towards entrants.[245] The ubiquity of presumptions has led a number of prominent commentators and judges to posit that most rules of law are little more than presumptions subject to rebuttal by the adversely affected party.[246] There are truly very few absolute principles in law.[247] Those principles that may appear to be absolute are in reality presumptions, which may be overcome in appropriate circumstances.[248] Arguably, the time has come for theoreticians and policy makers alike to reevaluate the present anti-globalist and globalist paradigms of cyberspace

---

240 *See* C. DONAHUE ET AL., CASES AND MATERIALS ON PROPERTY: AN INTRODUCTION TO THE CONCEPT AND INSTITUTION 291 (1974). For further information, see generally W. EMPSON, SEVEN TYPES OF AMBIGUITY (1930), and the extensive works of Owen Barfield including, in particular, OWEN BARFIELD, *Poetic Diction and Legal Fiction*, in THE REDISCOVERY OF MEANING, AND OTHER ESSAYS 44 (1977).

241 *See* McDonell-Douglas Corp. v. Green, 411 U.S. 792 (1973).

242 *See* GERALD GUNTHER & KATHLEEN SULLIVAN, CONSTITUTIONAL LAW (1998). Lon Fuller reminds us of many more examples, such as constructive delivery in contract law and implied provisions of contracts. *See* FULLER, *supra* note 148, at 8, 15.

243 Scores of studies were made on the nature of legal personality. For a handy bibliography of nineteenth-century foreign treatises, see Machen, *Corporate Personality*, 24 HARV. L. REV. 253, 254 n.3 (1911). *See also* John Dewey, *The Historic Background of Corporate Legal Personality*, 35 YALE L.J. 655 (1926); Sanford A. Schane, *The Corporation Is a Person: The Language of a Legal Fiction*, 61 TUL. L. REV. 563 (1987).

244 *See, e.g.*, Henry Maine, *Ancient Law, in* THE PROBLEM OF JURISPRUDENCE 371 (L. Fuller ed., 1946) (chapter reprints first half of HENRY MAINE, ANCIENT LAW (1861)). In referring to the fictions of Roman law, and to some of the older, jurisdictional common law fictions, Maine wrote, "The fact is in both cases that the law has been wholly changed; the fiction is that it remains what it always was." *Id.* at 370. Pound was the most expansive of all, including in his definition of legal fiction interpretation, equity, and natural law. *See* POUND, *supra* note 239, at 131; FULLER, *supra* note 148, at 53.

245 FULLER, *supra* note 148, at 53.

246 *See* Wilkinson, *supra* note 239, at 907.

247 *Id.*

248 *Id.* at 907-08.

and, ultimately, integrate territorial privacy into on-line privacy jurisprudence at large. Thus, the arguable recognition of on-line locales within their meaning in localist boundary theory could still comply with the physical world's notion of geographic spatiality: a configuration of multiple physical locales subject to a functional differentiation such as the public/private distinction.

C. *A Three Criteria Classification Scheme*

A fiction or a presumption, if it is to escape the charge of "erroneous conclusion" or "lie," must then comply with three requirements.[249] First, it must be be based on an inference justified by common experience, in the absence of other proof, and as drawn from available evidence.[250] Second, it must be phrased in realistic terms, namely an order, not an "inference." It should be designed as a disposition of the case in a certain contingency.[251] Lastly, it must be freely rebuttable.[252] This section will evaluate the application of these three conditions in cyberspace while overcoming the globalist and anti-globalist boundary claims in opposition to the possibility of legally acknowledging on-line locales.

1. Based on an Inference Justified by Common Experience

a. Absence of Other Proof

In the first of the two conditions, a fiction or a presumption must be based on an inference justified by common experience in the absence of other proof.[253] The lack of other proof does not have to be determined by the standard of certainty, but rather by a more relative test known as the substantial-evidence test.[254] Sometimes the reason for tolerating a gap either between evidence and findings, or between findings and decision, has to do with the limitations of human intellect or limitations on the magnitude of investigations that may be conducted in particular circumstances. In applying this standard, courts have already acknowledged that what is known and uncontradicted by empirical evidence may, in and of itself, be "substantial evidence" when first-hand evidence on the question is unavailable. This applies even in an analogous concern to cyberspace's spatial discourse, such as when upholding interstate commerce jurisdiction based on the evidentiary question of

---

249 FULLER, *supra* note 148, at 45.
250 *Id.*
251 *Id.*
252 *Id.*
253 *Id.*
254 *See, e.g.*, Fed. Power Comm'n v. Fla. Power & Light Co., 404 U.S. 453, 465-66 (1972).

how electricity actually moves in a bus.[255] However, not all propositions of fact that are useful and used in the administrative process are susceptible to proof with evidence.[256]

The globalist and anti-globalist boundary claims against the possibility of legally acknowledging on-line locales are rebutted here on two levels. The first weakness in the homogenous definition of space in its globalist boundary theory sense is counteracted by a form of heterogeneity involving the requirement of a physical presence. Arguably, localist boundary theory may overcome the physical world's wrong analogy, upheld as scientific truism, which suggests that locales and the nexus of individuals to them must be physical.[257] The second weakness of the homogenous globalist boundary theory that may be overcome by a form of heterogeneity involves the concern over discontinuities in the ability to interact between other spaces, namely the physical world, and other inner locations.[258] Applying localist boundary theory through a legal fiction of an on-line locale may arguably entail the existence of relations between locales without intrinsically involving geographical continuation, as will be explained herein.[259]

1) *First Heterogeneity: Physical Presence*

i. Non-physical Locality

In the real world, localist boundary theory is confronted with the erroneous notion that locales and the nexus of individuals to them must be physical. For a start, in regard to locales, we are told that although data has been traveling on wires and through the airwaves for centuries, the television, the telegraph, or the telephone are not "places" within which people travel.[260] In analogy to

---

255 *Id.*

256 *See, e.g.*, Fed. Power Comm'n v. Southern California Edison Co., 376 U.S. 205, 209 n.5 (1964); Travelers' Indem. Co. v. Parkersburg Iron & Steel Co., 70 F.2d 63, 64 (4th Cir. 1934); United States *ex rel.* Chapman v. FPC, 191 F.2d 796, 808 (1951), *aff'd*, 345 U.S. 153 (1953); *see also* 7 J. WIGMORE, EVIDENCE §§ 1917-1929, 1976 (3d ed. 1940 and Supp. 1970).

257 Thus, as explained in the outset of Part II, operationally, the extent of a territory can be defined by the set of points within it. *See* PETER HAGGETT, LOCATIONAL ANALYSIS OF HUMAN GEOGRAPHY 40-55 (1965). In non-physical environments, political geography allows us to uphold a one-point locale that, in essence, becomes non-physical. The emphasis on physical presence naturally originates in the physical world's application of localist boundary theory. *See* Farber, *supra* note 98, at 1270; Soja, *supra* note 99, at 53.

258 *See, e.g.*, DONNAN, *supra* note 105, at 9.

259 *Id.*

260 *See* ANDREW L. SHAPIRO, THE CONTROL REVOLUTION: HOW THE INTERNET IS PUTTING INDIVIDUALS IN CHARGE AND CHANGING THE WORLD WE KNOW 710-12 (1999) (cyberspace is not a real place but just a medium that we may control) [hereinafter SHAPIRO, THE Control Revolution]; Andrew L. Shapiro, *The Disappearance of Cyberspace and the Rise of Code*, 8 SETON HALL CONST. L.J. 703, 709, n.21 and accompanying text (1998); Timothy Wu, *When Law & the Internet First Met*, 3 GREEN BAG 2d 171 (2000).

previous telecommunications networks, most Internet users access the Internet through a dial-up modem which converts digital data to analog sounds that can be sent over a telephone line just like the human voice.[261] There were computer networks before the Internet that similarly relied on telephonic exchange of data.[262] Based on what is also a common view among post modernistic critical geographers concerning the notion of virtual space, space is not a container, but a medium in which "television space" is like "cyberspace": both do not exist as spaces, but instead as communications mediums.[263] In fact, support for the physicality of locales originates in public international law, which holds that even the smallest "area of land" must be "natural" land that is capable of legal appropriation.[264] Resembling cyberspace scientific truism, this pragmatic notion of locality seems to have led some public international law scholars in the physical world to insist that the islands must also be shown on geographical maps.[265] However, in not adopting a less pragmatic approach, the Anglo-American legal system has gradually and consistently acknowledged alternative non-physical forms of discontinuous localized spatiality in various constitutional contexts. In seminal First Amendment cases such as *Perry Education Ass'n v. Perry Local Educators' Ass'n*[266] and *Cornelius v. NAACP Legal Defense and Education Fund, Inc.*,[267] in the course of declaring locales non-public forums, the Court went on to identify the relevant locales—a school district's internal mail system and a charity fund drive among federal employees, respectively—notwithstanding that each "lacks a physical situs."[268] In another case,

---

261 For a discussion of the prevalence of private "bulletin board systems" in the late 1980s and early 1990s, see, for example, Debra B. Burke, *Cybersmut and the First Amendment: A Call for a New First Amendment Standard*, 9 HARV. J. L. & TECH. 87, 91-92 (1995).

262 *Id.*

263 SHAPIRO, THE CONTROL REVOLUTION, *supra* note 260, at 710-12 (for the legal perspective); Wu, *supra* note 260; *see also* EDWARD W. SOJA, POSTMODERN GEOGRAPHIES: THE REASSERTION OF SPACE IN CRITICAL SOCIAL THEORY (1989) (for the political geography perspective).

264 Article 121 of the Montego Bay Convention, December 10, 1982, uses a geological criterion, "a naturally area of land." Artificial islands are indeed excluded. Even here, however, the debates at the Third United Nations Conference on the Law of the Sea revealed the great complexity of this alleged pragmatic legal interpretation of locales. Thus, the nature of the area of land, and therefore the ability to use it, matters little. "Mud, slit, coral, sand, madrepore, rocks, etc. anything makes an island." MONIQUE CHEMILLIER-GENDREAU, SOVEREIGNTY OVER THE PARACEL AND SPRATLY ISLANDS 22 (Kluwer Law International 1996) (referring to LAURENT LUCCHINI & MICHEL VOELCKEL, 1 DROIT DE LA MER 331 (Pedone 1990)).

265 *See* CHEMILLIER-GENDREAU, *supra* note 264, at 22 (referring to GILBERT GIDEL, 48 LA MER TERRITORIALE ET LA ZONE CONTIGUË 137-278 (Recueil des Courts de l'Academie de Droit International, II, 1934)).

266 460 U.S. 37 (1983).

267 473 U.S. 788 (1985).

268 *Id.* at 801.

United States v. Grace,[269] the Court divided the Supreme Court grounds into perimeter sidewalks and interior grounds,[270] relying on the sidewalks' functional continuity with the adjoining streets,[271] and indistinguishability from other public walkways.[272] Constitutional criminal law also has transcended the notion that privacy is defined only by physical boundaries. In essence, the "public sphere" refers not to a locale as such, but to a fictitious sphere in which a set of activities constitutes a democratic society's self-reflection and self-governance. In a public sphere, private persons come together to discuss, deliberate, and decide public questions. Recognition of a fictitious locale was made functional. Any remaining doubts that such a functionally defined locale could qualify as a public forum were dispelled in *Rosenberger v. University of Virginia*,[273] where the Court characterized the university's student activity funding system as "open[ing] a limited forum,"[274] and declared that "[t]he SAF is a forum . . . more in a metaphysical than in a spatial or geographic sense, but the same principles are applicable."[275] With this jurisprudential shift in emphasis from what was perceived as a classic physical analysis towards a more functional one, locales are, indeed, apparent today as fora that do not always have to be physical gathering places.[276]

The notion of "territorial trap," as posited by the famous political geographer John Agnew, has been an important development in this respect. Agnew argues that territory in its traditional fixed and finite sense, as determined by rigid boundaries, should not be the focus for political geographical analysis. It is important not to fall into the trap of understanding territoriality as automatically entailing "the practices of total mutual exclusion which the dominant understanding of the territorial state attributes to it."[277] The legal

---

269 461 U.S. 171 (1983).

270 *Id.* at 179-80.

271 *Id.* at 180.

272 *Id.* at 179.

273 515 U.S. 819 (1995).

274 *Id.* at 829. The Court uses the term "limited" or "designated" forum to denote a forum that, at least for a class of speech that may be limited by speaker and/or subject matter, will be treated as a "public forum." *See id*; Int'l Soc'y for Krishna Consciousness, Inc. v. Lee, 505 U.S. 672, 678 (1992); *see also supra* Part II.A.2.

275 *See Rosenberger*, 515 U.S. at 830.

276 *Id.* (public place was regarded here in a "functional" form instead of a "geographic" one); *see also* Denver Area Educ. Telecomm. Consortium, Inc. v. FCC, 518 U.S. 727, 792 (1996) (Kennedy, J., concurring in part, dissenting in part).

277 David Newman, *From "Moribund Backwate" to "Thriving into the Next Centruy": Political Geography at the Turn of the Millenium* 3, *in* THE RAZOR'S EDGE: INTERNATIONAL BOUNDARIES AND POLITICAL GEOGRAPHY 57, 63 (Clive Schofield et al. eds., Kluwer Law Int'l 2002) (referring to J. AGNEW & S. CORBRIDGE, MASTERING SPACE: HEGEMONY, TERRITORY AND INTERNATIONAL POLITICAL ECONOMY 79 (1995)). Peter Taylor, also discusses alternative

concern involving accessibility to locales, therefore, would be the question of where access can be allowed, and what a would-be entrant can do with the information retrieved, instead of who should be eligible to access locales for collection purposes, as under or over-inclusively permitted by their lawful owners. Whenever such a functionally-based analysis is useful, there must be no inherent objection to why our legal system should not fictitiously expand the notion of locales into other virtual realms, particularly in cyberspace.

ii. Imperfect Geographic Nexus

The physical presence prerequisite has also been overcome in regard to the geographic nexus requirement. In the physical world, that predominantly has been the situation in environmental and land use cases before the federal courts where the issue was standing to sue.[278] Initially, in *Lujan v. National Wildlife Federation*, the Supreme Court required a "geographic nexus" between the injured plaintiff and the specific area endangered by agency action. The Court couched its argument regarding the nexus' degree of specificity in terms of "actually affected, without exhausting the forms of causality to physical ones."[279] In its discussion of the requirement of injury in *Lujan v. Defenders of Wildlife*, the Supreme Court intimated that the degree of specificity of the nexus requirement can be satisfied in many non-physical forms of causation: by a direct link between one's demonstrated work ("vocational nexus"), or interest in an endangered animal ("animal nexus"), or habitat ("ecosystem nexus") and an agency's pending action.[280]

Further non-physical expansion of the nexus' specificity followed in *Idaho Conservation League v. Mumma*[281] Distinguishing the National Wildlife Federation's specificity requirement, the Ninth Circuit held that the plaintiffs satisfied the "geographic nexus" requirement, despite their inability to specify threatened areas, be-

---

understandings of territory as they relate to the state and the organization of non-physical power in his rejection of the traditional physical notion of "territorial absolutism." *See id.* (referring to P.J. Taylor, *Territorial Absolutism and its Evasions*, 16 GEOGRAPHY RESEARCH FORUM 1 (1996)).

278 The nexus requirement originated in Flast v. Cohen, 392 U.S. 83 (1968). *See also* United States v. Richardson, 418 U.S. 166, 170 (1974); Linda R.S. v. Richard D., 410 U.S. 614, 618 (1973). *See generally* LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW §§ 3-17 (3d ed. 2000) (section 3-17, at 392-424, is of primary interest).

279 497 U.S. 871, 885-89 (1990); *see also* Sabine River Auth. v. United States Dep't of Interior, 951 F.2d 669, 675 (5th Cir. 1992) (quoting *Lujan v. Nat'l Wildlife Fed'n*, 497 U.S. at 876 (emphasis in the original)).

280 504 U.S. 555, 565-68 (1992).

281 956 F.2d 1508, 1517 (9th Cir. 1992); *see also Lujan v. Nat'l Wildlife Fed'n*, 497 U.S. at 882.

cause the proposed development areas had not yet been determined.[282] In their dissent in *Lujan v. Defenders of Wildlife*, Justices Blackmun and O'Connor further espoused and advanced the ecosystem nexus theory, acknowledging that "(m)any environmental injuries . . . cause harm distant from the area immediately affected by the challenged action . . . such as rivers running long geographical courses."[283] Likewise, the dissent impliedly endorsed the "animal nexus" theory in stating that the "environmental destruction may affect animals traveling over vast geographical ranges."[284] The imperfect nexus between geographically compact districts or locales and communities of interests was finally acknowledged in *Prosser v. Elections Board.*[285] In *Prosser*, the district court adopted its own apportionment plan for Wisconsin. Judge Posner found that there is not a complete correlation between geographical propinquity and community of interests.[286] In support of this imperfect nexus-requirement, the court, instead, warned against the possible results of rigid scientific truism, suggesting that the achievement of perfect contiguity and compactness would imply ruthless disregard for other elements of homogeneity. In addition, it would require breaking up counties, towns, villages, wards, and even neighborhoods.[287] In summary, with this jurisprudential shift in emphasis from what was perceived as a classic physical analysis towards a more functional one, locales and the physical nexus of individuals to them, indeed, are viewed today as interrelated fora that do not always have to be physical.

2) *Second Heterogeneity: Discontinuity*

The second weakness of the homogenous definition of space in its globalist boundary theory sense is threatened by a form of

---

282 *See Idaho Conservation* League, 956 F.2d at 1517 (upholding a geographic nexus requirement in the Forest Service); *see also* City of Los Angeles v. Nat'l Highway Traffic Safety Admin., 912 F.2d 478, 492-93 (D.C. Cir. 1990) (recognizing that persons suing to enforce National Environmental Policy Act requirements must show a sufficient geographical nexus to the site of a challenged project).

283 *Lujan v. Defenders of Wildlife*, 504 U.S. at 594.

284 *Id.* (citing Japan Whaling Ass'n v. American Cetacean Soc'y, 478 U.S. 221 (1986)).

285 793 F. Supp. 859, 861-62 (W.D. Wis. 1992).

286 28 U.S.C. § 2284 (1994).

287 *See Prosser*, 793 F.Supp at 286; *see also* Public Citizen v. United States Trade Representative, 822 F. Supp. 21, 28 (D.D.C. 1993) (citing United States v. Student Challenging Regulatory Agency Procedures, 412 U.S. 669, 687-88 (1973)) (rejecting the Government's argument that "many of the alleged environmental effects of the NAFTA on the U.S. Marine Mammal Protection Act are too widespread to be confined to a particular geographical location."). In support, the court in *Public Citizen* held that "the absence of a geographic nexus does not defeat a claim of standing because that 'would mean that the most injurious and widespread Government actions could be questioned by nobody.'" *Public Citizen*, 822 F. Supp. at 28.

heterogeneity involving discontinuities in the ability to interact between other spaces, namely the physical world, and other inner locations.[288] From a legal perspective, it entails the existence of relations between locales without intrinsically involving geographical continuation.[289] This lack of continuous homogeneity ultimately upholds the legal notions of territory and borders.[290] This is first achieved through the definition of territory, the political definition of a space that constitutes the core of geopolitical analysis.[291] It also weaves together a real and spatial analysis through the concept of a spatial system, a segment of space (real or hypothetical) which is formally and functionally organized through a patterning of attributes and a structuring of interactions. For example, a system of settlements or central locales would consist of locations tied together by certain shared or complementary attributes (i.e., size, proximate location, types of services performed, socio-cultural features) and the structuring of interactions between them (i.e., flow of money, influence, people, goods and information).[292] Second, borders are divided up by lawyers and geographers into the related concepts of boundaries and frontiers. More relevant to the easily demarcable potential locales in network environments—by IP addresses and gatekeeping technology—are boundaries (and thus boundary-making). These are the *lines* that demarcate territorial compartments, like states, urban neighborhoods, or group turfs, within which human activity takes place and is differentiated.[293] By drawing boundaries around space that they consider their own, people (and nations) strive to transform space

---

288 *See, e.g.*, *supra* note 99, at 9.

289 *Id.*

290 *See, e.g.*, DONNAN, *supra* note 105, at 9.

291 Haggett goes further to offer two separate human spatial patterns in his discussion of movement in space. He distinguishes between "fields," with undefined and indeterminate boundaries, and "territories," with specific boundaries. *See* Haggett, *supra* note 257, at 40-55. Thus, operationally, the extent of a territory can be defined in terms of control and occupancy, whereas field is defined in terms of movement, without the caveat of ownership. *Id.* In cyberspace, it is largely agreed that all websites (as potential locales) are owned, easily demarcable, and thus, at least theoretically could be subject to some level of control. Therefore, websites should be more closely related to the analysis of territories than that of fields. For further analysis, see also discussion *supra* Part III.C.2.

292 *See* Soja, *A Paradigm*, *supra* note 99, at 53.

293 *See* J.R.V. PRESCOTT, POLITICAL GEOGRAPHY 61-74 (Methuen & Co. Ltd. 1972); SUZANNE LALONDE, DETERMINING BOUNDARIES IN A CONFLICTED WORLD 8 (McGill-Queen's Univ. Press 2002); J.R.V. PRESCOTT, POLITICAL FRONTIERS AND BOUNDARIES 36 (London: Unwin Hyman 1987); L.K.D Kristof, *The Nature of Frontiers and Boundaries*, *in* The Structure of Political Geography: Theory and Applications 127 (R.E. Kasperson and J.V. Minghi eds., Aldine 1969); T. CRESSWELL, IN PLACE, OUT OF PLACE: GEOGRAPHY, IDEOLOGY AND TRANSGRESSION 149 (Univ. of Minn. Press 1996). In the physical world, with no appropriate analogy to network environments, "borderland" is then "the transition zone within which the boundary lies." PRESCOTT, POLITICAL FRONTIERS, *supra*, at 13-14.

into locales.[294] Such boundaries are described in words or treaties, shown on maps, or marked on the ground by physical indicators.[295]

In opposition to acknowledging both inner and outer borders in cyberspace, scientific truism, today, largely upholds that "in the strict technological sense,"[296] there is no empirical support for the spatiality paradigm,[297] and thus far, courts have failed to provide any.[298] Instead, a number of courts have made the mistake of overlooking the differences between the Internet and real space in a variety of contexts. For example, some courts applied the doctrine of trespass to chattels to email and website access, while assuming *inner* bordering.[299] Whenever Internet trespass cases create this analogy, courts have, in fact, only made a mistaken conceptual leap by assuming that cyberspace is a place in its traditional physical sense.[300] There also is not empirical support for the notion of cyberspace's "separateness" through *outer* bordering from physical space.[301] Nevertheless, these observations are minor from the individual's perspective of human behavior which legal truth regulates, regardless of the choice of legal fictions, on two levels. First, in the physical world, discontinuity is not an obstacle against the proprietariness concerning both the existence of proximity to locales upon their type and use. Notably, in public international law, in the history of claims over the intrinsic sovereignty of national groups to island territories, the argument based on geographical

---

294 *See* Stanley Waterman, *States of Segregation*, *in* THE RAZOR'S EDGE: INTERNATIONAL BOUNDARIES AND POLITICAL GEOGRAPHY, supra note 278, at 57, 63.

295 *Id.*

296 Hunter, *supra* note 97, at 472; Lemley, *supra* note 97.

297 *See* O'Rourke, *Property Rights*, *supra* note 97, at 592 & n.62 (referring to SACHS, *supra* note 143, at 1); Alfred C. Yen, *Western Frontier of Feudal Society?: Metaphors and Perceptions of Cyberspace*, 17 BERKELEY TECH. L.J. 1207, 1216 (2002).

298 *See* Hunter, *supra* note 97, at 472; Lemley, *supra* note 97.

299 For courts applying the doctrine of trespass to chattels to the Internet, see, for example, America Online v. Nat'l Health Care Discount, Inc., 174 F. Supp. 2d 890 (N.D. Iowa 2001); Oyster Software, Inc. v. Forms Processing, No. C-00-0724JOS, 2001 WL 1736382 (N.D. Cal. Dec. 6, 2001); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000); CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997); Intel Corp. v. Hamidi, 114 Cal. Rptr. 2d 244 (Ct. App. 2001), *rev. granted*, 43 P.3d 587 (Cal. 2002). For early use of the trespass doctrine to computers, see, for example, People v. Versaggi, 83 N.Y.2d 123, 129 (1994) (noting the New York state legislation proscribing computer trespass, title J, section 156.10 of the New York Penal Law Code). *But see* Ticketmaster Corp. v. Tickets.com, Inc., No. CV 99-7654, 2000 WL 525390 (C.D. Cal. Mar. 27, 2000); Express One Int'l, Inc. v. Steinbeck, 53 S.W.3d 895 (Tex. App. 2001).

300 *See, e.g.*, Hunter, *supra* note 97 (criticizing the courts' application of the cyberspace as place metaphor); O'Rourke, *Property Rights*, *supra* note 97, at 595-97 (criticizing courts for creating a broad property right on information for network environments); Burk, *supra* note 218, at 34 (criticizing courts for ignoring the damage requirement of trespass to chattels when dealing with cases involving network environments).

301 *See* O'Rourke, *Property Rights*, *supra* note 97, at 592 & n.62 (referring to SACHS, *supra* note 143, at 1).

proximity has never been recognized as constituting a rule of international law in favor of the state whose territory lies closest to the disputed islands.[302] In the physical world, these observations are also minor concerning the type and use of the neighboring locale. In fact, discontinuity between locales due to "spot zoning" or zoning ordinances, which create a small island of property with restrictions on its use different from those imposed on the surrounding property, are part and parcel of land use.[303] If it is of social and private interest to the parties involved in its use, and where there is a reasonable basis to treat the spot-zoned property differently from the surrounding property, spot zoning is valid.[304]

Like in the physical world, on-line territorial privacy could be upheld in private locales that are spotted inside publicly owned locales, such as public telephone booths,[305] women employees' public restrooms owned by their employer,[306] or public restrooms in skating rinks.[307] Arguably, there is no inherent justification to limit the recognition of discontinuity between fictional locales in cyberspace, where such have even less inherent physical constriction on access to present on-line locales based on gatekeeping technology, and their use by users in the first place.

Second, discontinuity can also be overcome by localist boundary theory based on analogous experience among network environments that predate cyberspace. In international monetary wiring networks, the format and order in which information is stored does not diminish its tangibility and logical retrieval whenever it is assembled and presented to the user as cohesive essence. There, the appropriate nature of data storage is also of marginal physical spatial relevancy. Instead, from the user's perspective, it is the interface through which data is accessed that is legally regulated, such as digitized money or other non-physical monetary rights. Both may be stored in one format, such as binary numbers that signify a sum of money at a bank account, or a check legal obligation that is

---

302 *See* MONIQUE CHEMILLIER-GENDREAU, *supra* note 264, at 27-29 & nn.20-23 and accompanying text.

303 *See* Little v. Winborn, 518 N.W. 2d 384 (Iowa 1994) (referring to Jaffe v. City of Davenport, 179 N.W. 2d 554, 556 (Iowa 1970)); *see also* 8 E. MCQUILLEN, MUNICIPAL CORPORATIONS § 25.84 (3d. ed., rev. 1991).

304 *See* Little v. Winborn, 518 N.W.2d. 384 (finding that determining whether there is a reasonable basis for spot zoning typically entails the consideration of the size of the spot zoned, the uses of the surrounding property, the changing conditions of the larger space, the use to which the subject property has been put, and its suitability and adaptability for various uses).

305 *See* Katz v. United States, 389 U.S. 348 (1967).

306 *See* Benitez v. KFC Nat'l Mgmt. Co., 714 N.E.2d 1002 (Ill. App. Ct. 1999).

307 *See* Harkey v. Abate, 346 N.W.2d 74 (Mich. Ct. App. 1983).

given in oral—but then accounted for per their interfacial appearance, which may then support functional discontinuity. In cyberspace, that interactive level of accessibility may, in fact, create a functional sense of distinguishable "placeness" in which meetings in cyberspace may become a viable alternative to meetings in physical space, regardless of the format and order in which information is stored.[308] In less than a "strict technological sense," legal truth already acknowledges that such normative discontinuities do not have to be inclusive in the cognitive sense; in fact, they can be fictional.

However, there are a few indications that a shift towards localist boundary recognition of virtual discontinuity is at reach. As recently as 1997, the Supreme Court acknowledged "that the creation of such [adult] zones can be constitutionally sound."[309] Instead of relaxing the discontinuous localist spatial analogy with the prevailing technocentristic globalist types of argumentation that tell us that geography ultimately implies both discrete locales and an ability to map their organization in either relation to the physical world or in separation from it, the Court understood that discontinuous zoning is more possible in cyberspace than in other media without adhering to a spatial relationship between all locales. Even in the midst of what the Court identified as technological uncertainty concerning future zoning abilities, Justice O'Connor's concurrence suggested that the Court was sensitive not only to how the Internet differed from any of the existing media offered as analogies at the present time,[310] but also to how the nature of the Internet might change over time in ways that affected its ability to be regulated.[311] Almost anecdotally, recognition of the homogenous weakness concerning continuity can ultimately be found within Johnson and Post's globalist argument. In fact, less attention has thus far been given to the fact that Johnson and Post's boundary approach normatively accepts the possibility of *inner* bordering within distinct cyberspace locales, "constellations,"[312] or "areas."[313] Each such virtual locale, as they normatively agree,

---

308 *See* Trotter Hardy, *Electronic Conferences: The Report of an Experiment*, 6 HARV. J.L. & TECH. 213, 215 n.3, 232-34 (1993) (discussing the advantages of e-mail conferences).

309 *See Reno v. ACLU*, 521 U.S. at 886 (O'Connor, J., concurring in the judgment in part and dissenting in part).

310 *Id.* at 889-90 (O'Connor, J., concurring in part).

311 *Id.* at 890 (O'Connor, J., concurring in part); *see also* Lessig, *supra* note 122, at 886-89. However, O'Connor's concurrence has been criticized as a rote application of the cyberspace as place metaphor. *See* Goldfoot, *supra* note 146, at 920-21.

312 Johnson & Post, *supra* note 114, at 1379 nn.92-96 and accompanying text.

313 *See id.* In a conversation with David Post, he further suggested that the "*inner* zoning" argument should have been understood as even more acute than the more cited "*outer*

could then likely develop its own set of distinct rules.[314] Thus, as localist boundary theory predicts, conduct acceptable in one locale of cyberspace could then be fenced-out by another.[315] Albeit, once again, based on a technocentristic approach, Johnson and Post's approach could succumb to the prospect of localist discontinuity as much as technology allows.[316] Thus, at least normatively, even Johnson and Post's strong globalist advocacy recognizes that localist heterogeneity in continuity could be sustained.

b. Drawn from Available Evidence

1) *Physical Distance: Remote Access*

According to globalist boundary theoreticians, the homogenous definition of space is threatened by heterogeneity due to the existence of distance[317] and its influence on entry preferences on individuals.[318] The presence of distance then assumes proportional proximity between locales, which then supports the preferences of either entering a given locale or otherwise observing it remotely.[319] Scientific truism rejects the soundness of these localist boundary theory propositions for cyberspace on several levels. First, whereas the ability to enter is assumed with a physical local, network environments are said not to have that ability because entering a website is physically impossible. Instead, only a replacement of data exists.[320] As Lemley all-purposely suggests, courts have not understood that no one "enters" websites.[321] Instead, in relevant on-line trespass cases, defendants merely send a request for information to a web server, which the plaintiff has made open

---

zoning separateness" argument vis-à-vis the physical world. Interview with David Post, I. Herman Stern Professor of Law at the Beasley School of Law, Temple University (March 12, 2004). Post's localist heterogeneous clarification, however, remains in tension with his main argument which views cyberspace as a global spatial system, regardless of its relation to the physical world spatiality.

[314] Johnson, *supra* note 114, at 1379.

[315] *See id.* at 1379, 1396-97.

[316] In further agreement with localist theory, Johnson and Post accept that a primary function and characteristic of such cyber borders or boundaries is its ability to be perceived by the one who crosses it. *Id.* at 1379 n.33 and accompanying text.

[317] Legal application of localist boundary theory to the concept of distance has, notably, given rise to the concept of frontiers. These are *zones* of varying depth, which marked either the political division between two countries, or the division between the settled and uninhabited areas within a country. PRESCOTT, POLITICAL GEOGRAPHY, *supra* note 294, at 54, 56-61; LALONDE, *supra* note 294, at 8; Kristof, *supra* note 294, at 127. Frontiers are of less importance to network environments, as will be explained herein.

[318] PRESCOTT, POLITICAL GEOGRAPHY *supra* note 294, at 54, 56-61; LALONDE, *supra* note 294, at 8; Kristof, *supra* note 294, at 127.

[319] PRESCOTT, POLITICAL GEOGRAPHY *supra* note 294, at 54.

[320] Lemley, *supra* note 97; *see also* Shapiro, *supra* note 119, at 710.

[321] *See* Joseph M. Olivenbaum, *Rethinking Federal Computer Crime Legislation*, 27 SETON HALL L. REV. 574, 577 (1997).

to the public, and the plaintiff's own server sends information in return.[322] Lemley further argues that the technological ability to sustain simultaneous usage through both multiple presences by one individual in various locales, and multiple presences by various individuals in one locale, is unique to network environments. As such, it entails further spatial disparity from the physical world's spatial analysis. To begin with, multiple entries/entrants are said to diminish the stability of locations.[323] In addition, it is said to override passage scarcity because for on-line communication purposes, bandwidth is effectively infinite.[324] Second, in a network environment, observance is said to be impossible because it lacks the concept of proportional proximity or a "next door" aspect.[325] Thus, as scientific truism argues, there can be no non-material public locales, such as streets or sidewalks, from which observation on either public or private spheres could be made possible.[326]

However, analyzing localist boundary theory as legal truth may lead us to different instrumental conclusions. In the absolute fictional sense, in consideration of territorial privacy, as Robert Post points out, privacy "cannot be reduced to objective facts like spatial distance or information or observance; it can only be understood by reference to norms of behavior."[327] Arguably, in the present case, scientific truism actually can be overcome partly from within cognition itself, as will be explained herein, so that the use of fiction is not indispensable. In the following regard, in some cases, legal fictions—far from being merely the metaphorical expressions of "norms"—are, in fact, tentative expressions of scientific truths, backed by legal values, to be discovered by the courts in their struggle to rationalize the subject matter presented to them.[328] Based on a conventional framework of legal fiction for on-line locales, an applied localist boundary theory for cyberspace could then aggregately support the existence of heterogeneity due to the existence of distance and its influence on entry preferences on individuals. This is so for reasons deriving from an analogy to the physical world's remote access and the added *reverse* remote access nature of cyberspace.

To begin with, in comparing non-physical electronic access to

---

322 Lemley, *supra* note 97.
323 *Id.* at 526.
324 *Id.*
325 *Id.*
326 *Id.*
327 Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 969 (1989); *see also* Solove, *supra* note 10, at 1129.
328 POUND, *supra* note 239, at 132.

physical access, there is still a sufficient level of scientific truth analogy that could permit us to overcome the obstacle set by this argument. This is achieved at two levels. First, the existence of non-physical entry should not be seen as unique to network environments, and thus, should be legally analogized to physical environments. In the latter, the requirement of actual trespass was largely abandoned with the tort of privacy intrusion.[329] For example, the requirement of a tangible entrance has been relaxed almost to the point of being discarded. Thus, for example, a single shot over private property was seen as trespass;[330] in different circumstances, parents were liable to a long-distance telephone company for trespass to personal property arising from their sons' unauthorized use of confidential codes to gain computer access to a company's system.[331] Other courts have held that microscopic particles[332] or smoke[333] may give rise to trespass, and the California Supreme Court has intimated that migrating intangibles (e.g., sound waves) may result in a trespass.[334] More relevant to cyberspace's digital setting was the precedent holding that electronic signals were sufficiently tangible to support a trespass cause of action.[335] Trespass analysis was not the only way through which courts have overcome the physical presence and entry requirements. Thus, in a constituting set of Federal Power Commission ("FPC") jurisdictional cases, as in the case of *Federal Power Commission v. Florida Power & Light Co.*,[336] the Court held that even a reaction up and down the line by a signal or a chain reaction is, in essence, electricity moving in interstate commerce.[337] The Court further held that no matter how small the quantity of the electromagnetic response, FPC jurisdic-

---

329 Nevertheless, there are some jurisdictions that still require actual trespass by the defendant. *See, e.g.*, Pierson v. News Group Publ'ns, Inc., 549 F. Supp. 635, 640 (S.D. Ga. 1982).

330 Portsmouth Harbor Land & Hotel Co. v. United States, 260 U.S. 327, 329-30 (1922) (holding a single shot across private property is a trespass); Herrin v. Sutherland, 241 P. 328, 331-32 (Mont. 1925) (holding that defendant, while standing on another's property, committed a trespass when he fired a shotgun over plaintiff's premises).

331 Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 473 (App. Dep't Super. Ct. 1996)

332 Bradley v. Am. Smelting and Refining Co., 709 P.2d 782, 788-89 (Wash. 1985).

333 Ream v. Keen, 838 P.2d 1073, 1075 (Or. 1992).

334 Wilson v. Interlake Steel Co., 649 P.2d 922, 924-25 (Cal. 1982).

335 *Thrifty-Tel*, 54 Cal. Rptr. 2d at 468; *see also* CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (stating that electronic signals or messages provide sufficient contact to give rise to action for trespass to chattels).

336 404 U.S. 453 (1972).

337 *Id.* at 458. Section 201 of the Federal Power Act owes its origin to the determination of the Court that a direct transfer of power from a utility in Rhode Island to a utility in Massachusetts is in interstate commerce. *See id.* at 458; *see also* Public Utils. Comm'n of R.I. v. Attleboro Steam & Elec. Co., 273 U.S. 83 (1927). Part II of the Federal Power Act is a direct result of *Attleboro*. *See* United States v. Public Utils. Comm'n of Cal., 345 U.S. 295, 311 (1953); Conn. Light & Power Co. v. Fed. Power Comm'n, 324 U.S. 515 (1945).

tion will attach because it is settled that Congress has not "conditioned the jurisdiction of the Commission upon any particular volume or proportion of interstate energy involved, and we do not . . . supply such a jurisdictional limitation by construction."[338] Where previously the tort often required the tortfeasor's presence in the private space, this proposal allows the presence requirement to be fulfilled virtually. It potentially expands the tort of unreasonable intrusion to include peering into private locales by the gathering of information by private persons using sense-enhancing tools.

In part, the tort of privacy intrusion may involve a purely sensory invasion, committed "by the use of the defendant's senses, with or without mechanical aids"[339] in order to oversee or overhear the plaintiff's private affairs, such as by looking into her upstairs windows with binoculars.[340] Thus, when a picture is taken of a plaintiff while she is in the privacy of her home, the taking of the picture may be considered an intrusion into the plaintiff's privacy just as remote eavesdropping or looking into her upstairs windows with binoculars are considered an invasion of her privacy.[341] Overall, most courts today do not require the physical penetration of private locales as an ingredient of spatial invasion of privacy. Wiretapping, bugging rooms with microphones, and peering into windows have all been held to constitute actionable intrusions.[342] Based on several updates and expansions of the Wiretap Act, the ECPA expanded the protection of privacy, prohibiting the unauthorized interception, use, and disclosure of information from remote access for both wire communications *and* electronic communications.[343]

Taking a picture or taping someone may sometimes have captured the data subject's privacy inside her locale by importing its content to ours, assuming that we remained in ours in the first place. Still, we say that even without leaving our locale, and only by the fact that we have captured data from another locale without

---

338 *Fla. Power & Light Co.*, 404 U.S. at 461; *see also Conn. Light & Power Co.*, 324 U.S. at 536; Pa. Water & Power Co. v. Fed. Power Comm'n, 343 U.S. 414 (1952).

339 *See* RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (1977).

340 *Id.*

341 *See* Hassman, *supra* note 17, at § 3(A).

342 *See* KEETON, *supra* note 16, at 854-55 (citing cases); *Id.* Some states have chosen to promote specialized types of privacy through targeted anti-paparazzi laws. *See, e.g.*, California's anti-paparazzi statute, CAL. CIV. CODE § 1708.8(b) (West 1999).

343 Electronic communications differ from wire communications in that they are communications that are not transmitted by sound waves and cannot be characterized as containing a human voice. Instead, they include telegraph, telex communications, electronic mail, nonvoice digitized transmissions, and the portion of video teleconferences that do not involve the hearing of voice or oral sounds. *See* 18 U.S.C. § 2510(12) (1988).

being there, an intrusion of privacy took place by "uploading" that captured data to our locale. In comparison with the physical world, the right analogy to network environments should be with *remote access* instead of *direct access*, as in some analogous physical environments. Such is the case with surveillance into a private locale from a public one, where invasion of privacy is done by technical surveillance that allows identification of private subject matter.[344] Cyberspace territorial privacy may arguably support an analogous proposition.

Alternatively, remote access can be made legitimate, and thereby has no intrinsic normative value. For example, remote access from a private locale into a public one, where, for instance, a naked woman has been observed with the use of binoculars and then identified while bathing at a public beach is considered legitimate. In both types of activities, remote access is seen to define liability, without remote access to spheres carrying physical presence or an intrinsic normative value per se. This interpretative rule also logically overcomes the separate scientific truisms' claim concerning multiple usages through both multiple presences by one individual in various locales, and multiple presences by various individuals in one locale. Therefore, multiple usage as either static presence or entry is not unique to network environments. Accordingly, it should not remain an obstacle in the sustainability of non-physical entry per se in non-physical environments, such as cyberspace.

In essence, the concept of territorial privacy is employed to govern the conduct of individuals who intrude in various ways upon one's life on-line. As in the physical world, in cyberspace, any gateway technology that could be seen as a public locale would avoid the risk of such illegal intrusion to any Internet user who makes the choice to enter upon sufficient notice of its public nature. Otherwise, for private locales on-line, namely private proprietary websites that would be acknowledged as such, intrusion into a user's private affairs would be illegal.

2) *Non-Physical Distance: Reverse Remote Access*

Second, and more specifically, this scientific truisms' argument can be mitigated by the unique nature of network environments per se. Whereas in the physical world the embedded assumption for any proof of the occurrence of entry is the space-

344 *See, e.g.*, Ass'n Servs., Inc. v. Smith, 549 S.E.2d 454, 459 (Ga. Ct. App. 2001); Miller v. Brooks, 472 S.E.2d 350 (N.C. Ct. App. 1996); Clayton v. Richards, 47 S.W.3d 149 (Tex. App. 2001).

shifting of relevant individuals through direct access, and only alternatively through remote access, a more particular type of space-shifting should be admitted in relation to cyberspace, namely reverse remote access. Technically, when a user clicks on a link, the user's computer sends a request to the server on which the desired document resides. That computer decides whether or not to respond favorably to the query.[345] It honors the request by sending a copy of the document to the user's computer, while the original remains on its server. In other words, the user who clicks on a link starts a chain of events that uses resources of both her system and those of the linked system. Commentators sometimes refer to this process as employing "pull" technology. Here, the user "pulls" a copy of desired content from the linked site rather than having that site's server "push" content indiscriminately to the user who may or may not be interested in it.[346] This type of information transaction from a given on-line locale to a user's computer may allegorically remind us of the popular Arab idiom, suggesting "If Muhammad cannot go to the mountain, let the mountain come to Muhammad." In both cases, space-shifting should then be considered functionally (and to some also theologically) appealing. Thus, whenever access to a given web page is made, an ISP sends the content of the requested data to the requesting user, and allows the latter to copy the content of that page as a temporary file.[347] Thus, instead of users moving between locales remotely, the locales move between the users remotely, and information gathering is done in the opposite order, but nevertheless remotely. As a result, users are allowed to search for and retrieve information stored in remote computers, as was also acknowledged as obiter

---

345 The collection of uncopyrighted identifiable data is not an act of unauthorized copying and would not be subject to the preemption section. Moreover, the assumption of both a permissible access and the use of temporary copyrighted "work of art" files, in their meaning in the Copyright Act, might override copyright preemption claims. In short, only when neither assumption applies in the case of copyrighted information, would the Copyright Act be the exclusive rule of decision under its preemption section. *See* Trotter Hardy, *The Ancient Doctrine of Trespass to Web Sites*, 1996 J. ONLINE L. art. 7, ¶ 2, 6.

346 *See* Jerry Kang, *Cyber-Race*, 113 HARV. L. REV. 1130, 1148 (2000) (explaining that surfing the Web is a common example of pull technology); *see also* Brief of Amici Curiae Law Professors, Bidder's Edge, Inc. v. eBay, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000) (No. 00-15995) (discussing "pull" technology and noting that "servers on the Internet are passive and do not deliver information to a consumer's computer unless that information is requested.").

347 Storing a web page in a cache constitutes copying. *See* MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511 (9th Cir. 1993); Advanced Computer Serv. v. MAI Sys. Corp., 845 F. Supp. 356 (E.D. Va. 1994); *see also* Raymond T. Nimmer and Patricia Ann Krauthaus, *Copyright on the Information Superhighway: Requiem for a Middleweight*, 6 STAN L. & POL'Y REV. 25, 32 (1994).

dictum by the *Reno v. ACLU* court.[348] Once the physical space-shifting requirement is inherently removed, remote access should be acknowledged in either direction. Only in cyberspace is access made remotely but in the opposite direction; otherwise, intrusion into *our* computers and observance of our digitized identities is practiced by locales, or some electronic parts of it, upon our earlier request.

Third, one should remember that the tort of intrusion only imposes liability for the use of one's senses if that person is using them in locales where she should not be. Thus, for instance, eavesdropping is allowed in a public locale. In *Nader v. General Motors*,[349] the court stated that "the mere observation of the plaintiff in a public locale does not amount to an invasion of the data subject's privacy."[350] Comment c to section 652B of the *Restatement* explains that a person who moves about in a public locale has emerged from seclusion, and thus, has opened herself up to observation by others.[351] However, under certain circumstances, surveillance may be so 'overzealous' as to render it actionable.[352] Thus, this general principle should not be understood to mean that all things that transpire in public are fair game for inquiry. In balance, as in the physical world, in the absence of a purposeful effort by some entity or device to actually track the actions of a particular individual, we would probably not consider social observation a form of monitoring.[353] Therefore, legitimate observation should not reveal information that people wish to hide.[354] The *Nader* court established that "[a] person does not automatically make public everything he does merely by being in a public place."[355] This conclusion should

---

348 *See generally* ACLU v. Reno, 929 F. Supp. 824, 834-36 (E.D. Pa. 1996) (specifying remote information retrieval as one of the common methods of communication on the Internet).

349 *See* 255 N.E.2d 765 (N.Y. 1970).

350 *Id.* at 771.

351 This was also upheld in *Dickson v. American Red Cross Nat. Headquarters*, No. 3:95-CV-2391-P, 1997 WL 118415 (N.D. Tex. Mar. 10, 1997) (granting motion for summary judgment and referring to K- Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632 (Tex. App. 1984)).

352 *See id.* (citing Pearson v. Dodd, 410 F.2d 701, 704 (D.C. Cir. 1969); Pinkerton Nat'l Detective Agency, Inc. v. Stevens, 132 S.E.2d 119 (Ga. Ct. App. 1963)).

353 *See* Rotenberg, *supra* note 174, at 22.

354 *See also* RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977) ("Even in a public place, however, there may be some matters about the plaintiff, such as his underwear or lack of it, that are not exhibited to the public gaze; and there may still be invasion of privacy when there is intrusion upon these matters.").

355 Nader v. Gen. Motors Corp., 255 N.E.2d 765, 771 (N.Y. 1970) ("[T]he mere fact that Nader was in a bank did not give anyone the right to try to discover the amount of money he was withdrawing."). One commentator has posited that the current formulation of the tort of intrusion does not extend protection to intrusions in public places, and that no case has ever expressly held otherwise. *See* McClurg, *supra* note 15, at 1085-86.

still be held valid when entry is done non-physically, as in cyberspace, and any recognition of remote entry should be done within this normative framework. In fact, in cyberspace, on-line anonymity is easily established and relatively cheap to achieve. Moreover, just like in the physical world, such identifiers are words or symbols that identify a specific person. Examples of identifiers within their meaning at the ECPA include an Internet customer's name, address, social security number, credit card number, and proof of Internet connection obtained by Internet providers.[356] As a result, observance and knowledge of a person's data identifiers should remain distinctive criteria in assessing privacy invasion on-line, even after territorial privacy is successfully integrated into cyberspace's privacy jurisprudence.

More particularly, on-line territorial privacy should not alter the explicit premise in Dean Prosser's statement adopted by the comments to the *Restatement (Second) of Torts*:[357] there is no difference between merely observing a person in a public locale and taking her photograph. Thus, in correspondence to the physical world, activities like wiretapping and broadcasting without identifying, based on material that was gathered in a public locale, should not amount to intrusion upon seclusion.[358] That legal framework should also now legitimize on-line non-identifiable data collection for purposes such as research on socio-economic trends or the development of statistics found in public locales. Such data collection could either be accomplished through real time observance, or "sensor technology," or just occasional observance of user's behavior in on-line public locales.[359]

Even more so, similar to the physical world, mere observation and/or legitimate data collection should then be legalized, notwithstanding whether the collection of observed data was made for commercial use or not. The physical world's law already admits

---

356 *See* 18 U.S.C. §§ 2510-2711 (2004); *see also* JOHN M. CARROLL, CONFIDENTIAL INFORMATION SOURCES: PUBLIC & PRIVATE 10-12 (2d ed. 1991); RAYMOND T. NIMMER, THE LAW OF COMPUTER TECHNOLOGY §§ 13.07, 16.09 (2d ed. 1992) (Raymond Nimmer also mentions more specific identifiers: individual eligibility for government benefits, qualifications for employment, criminal records, draft records, real estate transactions, marriage, birth and death records, automobile registration, and tax liability).

357 *See* KEETON, *supra* note 16, at 855-56; RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977).

358 *See* RESTATEMENT (SECOND) OF TORTS § 652B (1977).

359 *See* NIMMER, *supra* note 357, § 16.09. For such important web-based applications, such as telemedicine, data visualization, data-mining, and distance learning, see, for example, CITRIS.Net projects, available at http://citris.ucdavis.edu/citrisnet.html (last visited Apr. 14, 2005), and Continuous Output and Navigation Technology with Refinement On-Line (CONTROL) projects, available at http://control.cs.berkeley.edu (last visited Apr. 11, 2005).

such circumstances. For example, in *Deteresa v. American Broadcasting Companies, Inc.*,[360] the court found that under California law, a television producer's conduct in arranging for surreptitious videotaping of a woman in public view by a camera person in a public place, and in broadcasting only a five-second clip of the tape without broadcasting the woman's name or address, had an insubstantial impact on privacy interests and would not support the woman's intrusion into a seclusion privacy claim.[361] Accordingly, it is uniformly held that the use of a photograph of a person's property does not constitute an invasion of that person's privacy justifying recovery unless that person's identity is apparent from the photograph.[362] In other words, invasion of privacy by taking someone's picture, even for commercial use, is not possible unless the picture tells the person's identity.[363] For example, when a photograph of the plaintiff's property has been used by the defendant in an advertisement, the plaintiff's identity must be apparent in the photograph.

2. Phrased in Realistic Terms

a. Implicit Individual Consent

Within localist boundary theory, recognition of a distinct legal status of locales requires that individual consent and cost of control match the particular functions on the whole sub-segment of types of locations, namely private and public. A legal fiction of on-line locales can arguably be easily phrased in realistic terms in compliance with both conditions. For a start, it could allow individual implied consent to on-line data collection. In public locales, Dean Prosser's conclusion that there cannot be an intrusion in a public locale depends upon the acceptance of two supporting premises, one implicit and one explicit. The implicit premise is that one assumes the risk of public inspection when she ventures into a public place.[364] This assumption of risk analysis is clearly discernible in *Gill v. Hearst Publishing Co.*,[365] a famous privacy case relied upon by Dean Prosser as support for his comments regarding the absence of privacy in public locales.[366] The court based much of its reasoning on an assumption of risk analysis. The court commented that

---

360 *See* 121 F.3d 460 (9th Cir. 1997).
361 *Id.*
362 RESTATEMENT (SECOND) OF TORTS § 652B (1977).
363 *See* CARROLL, *supra* note 357, at. 11-12.
364 RESTATEMENT (SECOND) OF TORTS § 652B (1977).
365 253 P.2d 441 (Cal. 1953).
366 *See* Prosser, *supra* note 10, at 391 n.81.

the plaintiffs were "in a pose voluntarily assumed in a public market place,"[367] that they "had voluntarily exposed themselves to public gaze in a pose open to the view of any persons who might then be at or near their place of business,"[368] that "[b]y their own voluntary action plaintiffs waived their right of privacy so far as this particular public pose was assumed,"[369] and that the plaintiffs' right of privacy ceased by "their own voluntary assumption of this particular pose in a public place."[370]

However, in private locales, as the *Restatement* provision initially recognized, to find true consent, the plaintiff must have full knowledge of the risk and voluntarily choose to encounter it. In order for an Internet customer to have a reasonable expectation of privacy in her personal information under the risk-analysis approach to the Fourth Amendment,[371] the data must not be knowingly exposed to others,[372] and the Internet service provider's ability to access data must not constitute disclosure.[373] That expectation of privacy can be applied to private locales intruded by private data collectors. Moreover, as in the physical world, when an on-line business is available to the public, a would-be entrant to the on-line locale in a given website—at a reasonable time and in a reasonable manner—would have the implied consent of the owner to be there; as long as the person engages in any acts consistent with the purposes of the business or locale, there would be no trespass.[374]

Practically speaking, should the courts choose this path based on on-line territorial privacy and the following construction of on-line locales, affected website owners would be prohibited from freely disclosing their members' identities and relieved from the need to attest to contractual consent in both types of locales. Therefore, they would be required only to give adequate notice. As already acknowledged by the FTC, the notion that choice should be respected is almost universally accepted as a starting

---

367 *Gill*, 253 P.2d at 444.

368 *Id.*

369 *Id.*

370 *Id.*

371 Assumption of risk is an affirmative defense that could be used by data collectors in cyberspace to claims based upon negligent or reckless conduct of their part. *See* RESTATEMENT (SECOND) OF TORTS § 496A (1977).

372 U.S CONST. amend. IV.

373 *See* RESTATEMENT (SECOND) OF TORTS § 496C(1) (1977).

374 *See* Mosher v. Cook United, Inc., 405 N.E.2d 720, 721 (Ohio 1980) (labeling a comparison price shopper a "business invitee" subject to the property owner's right to revoke the shopper's license at will); 25 AM. JUR. 2D *Trespass* § 48 (1989 & Supp. 2000).

point for practical reasoning for privacy regulation.[375] However, such an invitation presupposes that the conduct of would-be entrants will be in-line with the nature of the locale.[376] In a zoned cyberspace, boundaries would then serve as signposts that provide warning that we will be required, after crossing, to abide by different privacy rules. Thus, a link to a notification about information collection, or a built-in disclaimer into the website's locale or several locales, would have to appear in response to every search or directory listing that included the target. It would also have to attract the attention of a user seeking a specific address out of a potentially long list of related sites. Thus, all that would actually be required is one of the following: either the insertion of a command into the web page that opens a page maintained by the access-seeker on her own server as a separate window, or a built-in disclaimer into the website's locale or several locales, in the visitor's browser.[377]

As with other precise legal fictions, the risk of over-inclusive distinctions between locales through the simple measurement of disclaimers may entail a regulatory paradox. The more it strives to grasp and define the essence of a legal proposition, such as the existence of on line spatiality, the more we may get to promote its declared legal purposes. Courts should initially confine themselves to determining whether law and justice require or permit a change in the status quo. To decide, courts should look to what practices, policies, procedures, and agreements exist in the locale that may or may not create a reasonable and legally enforceable expectation of privacy.[378] Information privacy cases can be analogous. In such cases, courts have found that when employees used a lock, password, or encryption to protect certain items, that action created an "expectation of privacy" that could be violated when companies

---

375 *See* Gavison, *supra* note 1, at 441. The FTC has interpreted the norm of choice so as to include making a choice among a number of alternatives. *See* FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 17 (1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf (last visited April 11, 2005).

376 See *Mosher*, 405 N.E.2d at 721; 25 AM. JUR. 2D *Trespass* § 48, *supra* note 375.

377 Using JavaScript, the following would open a window titled *CyberSidewalk* at the site www.sidewalkspeaker.org: <SCRIPT> CyberSidewalk=window.open ("http://www.sidewalkspeaker.org")</SCRIPT>. A web page can be broken down into the information transmitted by the web server and the resulting translation achieved by the browser software. Thus, the static "page" that one sees on the monitor is achieved by the browser's response to a series of instructions contained in the Hypertext Markup Language ("HTML") "page" transmitted by the server. *See* Rajesh Vijayakumar & Devi S Nadh, *A Beginner's Guide to JavaScript, at* http://www.javascriptguide.com (last visited Apr. 14, 2005) and Netscape Assistance, *An Exploration of Dynamic Documents, at* http://home.netscape.com/assist/net_sites/pushpull.html (last visited April 11, 2005).

378 SHARON K. BLACK, TELECOMMUNICATIONS LAW IN THE INTERNET AGE 315 (2002) (applying this proposition to the information privacy category).

break the lock, password, or encryption.[379] A similar comparison could be made by courts to territorial privacy when users act to hide non-identifiable data upon entry to public locales. Morevover, upon entry to private locales, website owners may legitimize their collection activities by clarifying that the website owner collecting such data may override identity concealment measurements used by would-be entrants to such locales.[380]

b. Proportional Cost of Control

Recognition of distinct locales also requires that the cost of control should match the particular functions on the whole subsegment of types of locations, namely private and public. Based on information privacy analysis, the legal problem will likely be the detection of "trespasses" or the unauthorized use of an informational work.[381] As noted earlier, practical problems exist with policing very long borders of real property, but they seem to pale in comparison to the problem of detecting "trespass" activities like unauthorized copying or unauthorized uses of informational works.[382] If these costs are excessive in cyberspace, one might argue against a private-property regime because such a regime may not be "worth it."[383]

However, based on an acknowledgment of territorial privacy, there should be a difference between control over content use, as assessed through information privacy protection, and control over access. Territorial privacy would only need to uphold sufficient control over access. Even when control over access derives from ownership, the law generally gives owners of real property the right to exclude others from entrance, regardless of whether or not the intruder causes harm.[384] Thus, the doctrine of trespass to chattels traditionally required actual harm to the chattel, while trespass to land was actionable whether or not the owner's interest in the land was injured.[385] However, according to the the tort of intrusion

---

379 *Id.* at 315; *see also* Hardy, *supra* note 97, at 247.

380 *Id.*

381 *See* Hardy, *supra* note 97, at 247.

382 *See id.*

383 *See id.*; *see also* David McGowan, *Website Access: The Case for Consent*, 35 LOY. U. CHI. L.J. 341, 373 (2003) (presenting a utilitarian analysis of on-line access policy).

384 For the context of trespass, see RESTATEMENT (SECOND) OF TORTS § 218 cmt. e (1965); *see also* KEETON, *supra* note 16, at 67 (outlining the historical cause of action in trespass).

385 *See* KEETON, *supra* note 16, at 67. For the context of trespass analysis in cyberspace, see Intel Corp. v. Hamidi, 71 P.3d 296, 304 (Cal. 2003). *Intel Corp.* held that "[w]hile one may have no right temporarily to use another's personal property, such use is actionable as a trespass only if it 'has proximately caused injury' to the property in question." *Id.* at 306

upon exclusion, a similar presumption to that of trespass of land exists in the case of privacy invasion. Invasion is intrinsically foul, even with no harm, because it is an "interference tort" as opposed to a "damage tort" where the proof of harm is necessary following the proposition of "no harm, no foul." Gavison further argues that in terms of social norms, privacy "is simply a conclusion, not a tool to analyze whether a certain invasion should be considered wrong in the first place."[386] In other words, an intrusion on privacy is intrinsically harmful because it is defined as that which injures social personality.[387] Thus, the tort of invasion of territorial privacy is qualitatively similar because the injury at issue is logically entailed, rather than merely contingently caused, by improper conduct.[388]

In contrast to the usual cause of action for negligence, this privacy tort enables a plaintiff to make out her case without alleging or proving any actual or contingent injury, such as emotional suffering or embarrassment.[389] With this lowered standard of proof of infringing behavior, website owners should have the right to exclude others from gaining access to their information on a territorial basis, even if their entry does not harm the site in any way.[390] Consequently, privacy norms against intrusion could be upheld more easily in cyberspace, especially given the fact that surveillance technology only makes an illegal collection of information easier and cheaper to attain.

Notably, in tort law, a full level of control by owners is only required in private locales. Alternatively, any lack of a sufficient level of actual control does not negate the concept of spatiality at large, rather, only the possibility that such locale may be constituted as a private one. As in physical world jurisprudence, virtual spatiality framed as public, may still be upheld.[391] In such cases, the legal standard for spatiality could still constitute an on-line public locale, just like in the physical world.

(quoting Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 473 (Ct. App. 1996)); Burk, *supra* note 218, at 48-49.

386 *See* Gavison, *supra* note 1, at 426 n.18.

387 *Id.*

388 *See* Post, *supra* note 328, at 964; Gavison, *supra* note 1, at 425-40.

389 *See* Post, *supra* note 328, at 964.

390 *See* O'Rourke, *supra* note 97, at 587. For the difference between "damage" torts and "interference" torts, see Post, *supra* note 329, at 964 n.42 and accompanying text.

391 *See, e.g.*, Shulman v. Group W Prods., Inc., 955 P.2d 469, 490 (Cal. 1998) (holding that filming a rescue attempt at an accident scene, fifty feet down an embankment of an interstate highway, was not an invasion of plaintiff's privacy); *see also* Salazar v. Golden State Warriors, 124 F. Supp. 2d 1155 (N.D. Cal. 2000). There, the California Supreme Court stated there is no invasion of privacy into a private sphere where plaintiff had no actual control of the premises where the incident took place, consequently upholding the default existence of a public sphere.

3. The Presumption Has to be Either Conclusive, or Freely Rebuttable

Presumptions or legal fictions of on-line locales can be made either conclusive or rebuttable. First, and proper to the legal fiction of on-line locales, they should be made conclusive presumptions which are substantive rules of law.[392] Conceptually, following Gray's classification scheme of legal fictions (borrowed from Ihering), legal fictions, in fact, are broken down into "historic," or procedural, fictions and "dogmatic" fictions.[393] Accordingly, dogmatic fictions should never be used to change the law, as the historic fictions were used in the past. Instead, they should only be used for the purpose of classifying established rules, such as the existing private/public distinction between locales in the physical world. In that regard, the legal fiction of on-line locales should merely be regarded as applicative and as a direct and inevitable continuation of locales in the physical world. Consequently, one should be able to state the real doctrine for which they stand.[394] Ultimately, the legal necessity for an adequate technical vocabulary makes it desirable that well-founded fictions, such as on-line locales converted into legal truths, would be picked with appropriate judicial discretion.[395]

Regulators should be attentive to the reality that like other legal fictions, on-line locales are founded in part upon exceptionally strong and visible policies which have been said to persist despite proof rebutting their factual basis.[396] That is why the other type of presumption, namely, the rebuttable presumption, should not be preferred in the construction of on-line locales. Instead, rebuttable presumptions are rules of law that attach to proven evidentiary facts and certain procedural consequences as to the opponent's duty to come forward with other evidence.[397] As explained before, communication mediums such as cyberspace are not susceptible to the possibility of rebutting physical spatiality, as such is not assumed to be present in the first place. As a result, on-line locales should not be seen as an "inference" or a dissimilarity, which is subtle but not unreal. As unreal constructions, on-line locales are not "conclusion[s] which the [trier of fact] is *permitted*, but not

---

392 *See* WIGMORE, *supra* note 256, § 2492; MCCORMICK, EVIDENCE § 342, at 804 (2d ed. 1972).

393 *See* J. GRAY, THE NATURE AND SOURCES OF LAW 30-37 (1921).

394 *See id.* at 37.

395 *See* FULLER, *supra* note 148, at 23.

396 *See* MCCORMICK, *supra* note 393, § 345, at 822-23.

397 OLIN GUY WELLBORN III, THE RULES OF EVIDENCE: CASES AND MATERIALS 553 (West 2000).

compelled to draw from the facts."[398] Instead, as real presumptions (also referred to as presumptions of law) on-line locales should be made as an inference through which the law directs the trier of fact to functionally draw if it finds a given set of justifications. The content of such on-line locales would then serve policy makers to specifically distinguish on-line public locales from the present unbalanced default mosaic of on-line private allotments. Public locales could then be held conclusive for newsgroups,[399] in pre-print archives of article environments enabling scientists to share the latest learning in their fields,[400] and web resources on the poster's favorite topic.[401]

SUMMARY AND CONCLUSIONS

Thus far, cyberspace has not been left with a public sphere and public locales, nor has a balanced privacy policy been established. Instead, only a *private* and overly broad legal rule of privacy has been adopted. Thus, database protection against the various forms of information collection, and particularly registration data that is collected upon initial entry to databases, is arguably an overgeneralized privacy category. It includes both possible public and private on-line locales, while overly protecting the former.

This study shows that notwithstanding information or database privacy jurisprudence, territorial privacy and private and public locales, more specifically, could coexist on the Internet, just as they do in the physical world. In accordance with previous jurisprudential developments, privacy should continue to be valued instrumentally. Courts may then be required to differentiate and identify private locales and then separate them out from public ones. Thus, a legal fiction of on-line locales should now be constructed for cyberspace's overall privacy policy.[402]

In public locales, privacy protection should be balanced with protecting legitimate observance and non-identifiable data collection either directly (collecting registration and transactional data) or indirectly (collecting clickstream data) by websites. Notably, in regard to databases, most information collection and use occurs in what would otherwise be considered public, and as argued, many

---

398 Bray v. United States, 306 F.2d 743, 747 (D.C. Cir. 1962) (emphasis added).

399 *See, e.g.*, Slashdot, *at* http://slashdot.org (last visited April 11, 2005).

400 *See, e.g.*, Los Alamos Physics Preprint Server, *at* http://www.arxiv.org (last visited April 11, 2005).

401 *See, e.g.*, Archinect: Architectural and Urban Planning Sites, *at* http://www.archinect.com (last visited April 11, 2005).

402 *See, e.g.*, Shapiro, *supra* note 96 (in justification of the First Amendment "public forum" doctrine); Goldstone, *supra* note 96, at 3.

parts of cyberspace may well be considered public locales. Moreover, database protection falls short in applying information privacy whenever an otherwise potential locale would include multiple databases. Therefore, identifying such databases as private or public locales, may also avoid over-fragmentation of these regulatory subject matters. Indeed, for the physical world, courts have accepted claims involving territorial intrusion whenever the category of privacy that would likely be infringed was made in regards to databases and would, therefore, belong to the category of information privacy.

Nonetheless, in cyberspace the United States government, and primarily the FTC's privacy policy, still encourage the withdrawal of law as a balancing constraint. This is demonstrated by the FTC's stance toward online website privacy which emphasizes both technological and market self-regulation for the adoption of privacy policies. However, as shown, technology alone has thus far failed to provide protection comparable to that which could be provided with the intervention of law. Technology has simply been incapable of establishing a comprehensive boundary solution by itself.

A legal fiction of on-line locales can arguably be phrased in realistic terms in compliance with all-purpose territorial privacy protection. For a start, it could allow individual implied consent to on-line data collection. That expectation of privacy can further be applied to private locales. Moreover, as in the physical world, when an on-line business is open to the public, a would-be entrant to the on-line locale in a given website—at a reasonable time and in a reasonable manner—would have the implied consent of the owner to be there; as long as the person engages in acts consistent with the purposes of the business or locale, there would be no illegal intrusion.

More particularly, territorial privacy on-line should not alter the explicit premise in Prosser's statement that has been adopted by the comments to the *Restatement (Second) of Torts*,[403] that there is no difference between merely observing a person in a public locale and taking that person's photograph. Thus, as in the physical world, activities like wiretapping and broadcasting using material that was gathered in a public locale, without identifying, should not amount to intrusion upon seclusion. As shown, that legal framework should also now legitimize on-line non-identifiable data collection for purposes such as research on trends or the develop-

---

[403] KEETON, *supra* note 16, § 117, at 855-56; RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977).

ment of statistics in public locales. This can be done either through real time observance through sensor-based technology or occasional observance of user's behavior in public locales on-line.

Even more so, just like in the physical world, mere observation and/or legitimate data collection in on-line locales should be seen as legal, notwithstanding whether the collection of observed data was made for commercial use. The physical world's law already admits such circumstances. As a practical matter, observance in private locales should be replaced through a mechanism of voluntary disclosure of whatever types of information, namely transactional, registration, and clickstream data, which would be abided to by would-be entrants in public locales. Observance should be freely allowed, as long as a notice of the public locale is made known. However, it should be solely restricted to the collection of non-identifiable registration and clickstream data.

Legitimate observation should not reveal data identifiers that people wish to hide. Similar to the physical world, such identifiers are words or symbols which identify a specific person. As a result, observance and knowledge of a person's data identifiers should remain distinctive criteria in assessing privacy invasion on-line, even after territorial privacy is successfully integrated into cyberspace's privacy jurisprudence. This conclusion should still hold true when a non-physical entry is made, as in cyberspace; any recognition of remote entry should be evaluated within this normative framework.

Moreover, any lack of a sufficient level of actual control should not negate the concept of spatiality at large, rather it should only negate the possibility that such spatial location may be constituted as a private sphere. Notably, in tort law, full level of control by owners is only required in the private sphere. Like in physical world jurisprudence, a lesser level of control in virtual spatiality framed as a public sphere may still be upheld. In such cases, the legal standard for spatiality could still constitute an on-line public sphere.

As with real presumptions, also called presumptions of law, on-line locales should be made as an inference through which the law directs the trier of fact to functionally draw only if it finds a given set of justifications. The content of such locales would serve policy makers to specifically distinguish public locales from the present unbalanced default mosaic of on-line private allotments.

Ultimately, like in the physical world, whether the ownership of public locales is public, private, or a combination of the two, on-line public locales will finally legitimize a territorially-based collec-

tion of taxes, the enforcement of criminal and First Amendment policies, and even the possible use of copyrighted information distributed through the public sphere.