

THE CASE OF ON-LINE TERRITORIAL PRIVACY

**Law, Geography and Cyberspace:
The Case of On-Line Territorial Privacy***

By: Daniel Benoliel**

TABLE OF CONTENTS

I. Introduction.....	4
II. Cyberspace boundary discourse: The two approaches.....	12
A. Globalist boundary theory: Johnson & Post and Lessig.....	14
B. Anti-globalist boundary theory: Hunter and Lemley.....	18
III. The Localist boundary synthesis: A legal fiction of on-line locales.....	20
A. Overview.....	20
B. The Epistemological framework.....	20
1. Recognition of utility, or.....	20
a. Lack of distinctive locales.....	21
b. The insufficiency of technological solutions.....	24
c. The sufficiency of legal solutions.....	27
2. Consciousness of falsity.....	29
C. A three criteria classification scheme.....	33
1. Based on an inference justified by common experience.....	34
a. Absence of other proof.....	34
1) First heterogeneity: Physical presence.....	35
i. Non-physical locality.....	35
ii. Imperfect geographic nexus.....	37
2) Second heterogeneity: Discontinuity.....	38
b. Drawn from available evidence.....	42
1) Physical distance: Remote access.....	42
2) Non-physical distance: Reverse remote access.....	46
2. Phrased in realistic terms.....	49
a. Implicit individual consent.....	49
b. Proportional cost of control.....	51
3. The presumption has to be either.....	52
a. Conclusive, or.....	52
b. Freely rebuttable.....	52
VI. Summary and conclusions.....	54

THE CASE OF ON-LINE TERRITORIAL PRIVACY

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 governmental intrusion, and “non-private” places, in which the individual does not have a recognized expectation of privacy. The designation of an area as “private” then also protected the personal information located there from governmental seizure. In the real 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, was not left with a public sphere nor has a balanced territorial privacy policy so far been established. Instead, based on the category of database privacy protection, only an ownable-based 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 real world is subject to a default rule of a continuous public sphere that 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 regulated according to telecommunications and antitrust law, the present default rule contains a mosaic of private allotments – namely, neighboring proprietary web sites.

This anomaly is even more acute given that the U.S government, the FTC and theoreticians alike, thus far, have developed neither comprehensive nor supportive boundary theory that could maintain territorial privacy. All three, instead, have implicitly or explicitly only considered technocentric 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, indeed, could construct a legal fiction of on-line locales, through which territorial privacy, ultimately, could be integrated into cyberspace privacy policy at large.

I.
INTRODUCTION

Privacy has always been a challenging legal concept and is difficult to define.¹ It has no single interest, but rather has several different dimensions or categories that are not just observed but also legally constructed. Predominantly, the concept of privacy can generally be divided into four categories.² The first 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. Law, originally, provided a remedy solely for physical interference with the life and property of the individual.³ The second is 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.⁴ It covers the various interests of individuals in communicating among themselves using various forms of communications. The third is information privacy, which concerns the control and handling of personal data.⁵ 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*⁶ and *Roe v. Wade*.⁷ The fourth, and the focal point of this study,

* © 2004 Daniel Benoliel

** J.S.D. candidate and a John M. Olin Fellow, UC 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 was also awarded best article in the 14th Annual Computers, Freedom & Privacy Conference student paper competition. For their most helpful comments and support, I am indebted to Pamela Samuelson, Mark Lemley, David Post, Dan Hunter, Julie Cohen, Edward Soja, 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.

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, 34 (1967); Raymond T. Nimmer, *Information Law, Privacy Right vs. Public Right* (November 2001), ¶ 8:31.

² See, e.g., Ruth Gavison, *Id.*, at 433; Joseph I. Rosenbaum, *Privacy on the Internet: Whose Information is it Anyway?*, 38 *Jurimetrics* 565, 566-67 (1998). See, discussion herein.

³ 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, also, 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 (1977), at 266 & n.119.

⁴ See, e.g., *Bartnicki v. Vopper* 532 *U.S.* 514, 526 (2001); *U.S. v. McRae*, 156 *F.3d* 708, 711 (6th Cir. 1998); *Kee v. City of Rowlett*, 247 *F.3d* 206, 216-17 (5th Cir. 2001).

⁵ Ruth Gavison, *supra* not 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).

⁶ 381 *U.S.* 479 (1965)

⁷ 410 *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'. See, also, *Whalen v. Roe* 429 *U.S.* 589 (1977), where using a spatial metaphor, Court reaffirmed that constitutionally protected "zone of privacy" jointly protected the "individual interest in

THE CASE OF ON-LINE TERRITORIAL PRIVACY

is territorial privacy, which involves setting limit boundaries on intrusion into an explicit space or locale.⁸ Turning our focus from disruptions to the practices, which they disrupt, we often refer to aspects of these practices as "private matters." In other words, we say that certain things, places, and affairs are "private."⁹ Initially, Courts designated two classes of excluded areas: "private" areas, as a home,¹⁰ or a reserved hotel room,¹¹ in which the individual can expect to be free from governmental intrusion¹² and "non-private" areas, in which the individual does not have a recognized expectation of privacy.¹³ The designation of an area as "private" protected the personal information located there from intrusion and governmental seizure. The Restatement (Second) of Torts most notably incorporated these views *into* the comments to section 652B,¹⁴ which defines the privacy tort of intrusion.¹⁵ Thus, Courts 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.¹⁶ On a public street, or in any other public place, the plaintiff has no legal right to be alone;¹⁷ the circumstances themselves in such cases are not secluded,¹⁸ and it is not an invasion of her privacy to do no more than follow her about and watch her there.¹⁹

avoiding disclosure of personal matters", with the individual's "independence in making certain kinds of important decisions". *Id.* at 599-600.

⁸ In boundary theory, the terms 'space', 'locale' and 'sphere' or 'area', have separate spatial meanings that would be distinguished later on. See discussion, in Part II, herein.

⁹ See, e.g., William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383, 389 (1960), at 390-91; Daniel J. Solove, *Conceptualizing Privacy*, Calif. L. Rev. 1087 (2002), at 1130 [Hereinafter, 'Solove, Conceptualizing Privacy']. See, also, John Stuart Mill, *On Liberty* 11-13, 75-77 (Norton ed. 1975) (emphasizing public and private locales).

¹⁰ *Clinton v. Commonwealth*, 130 S.E.2d 437 (Va. 1963), rev'd, *Clinton v. Virginia*, 377 U.S. 158 (1964)).

¹¹ *Stoner v. California*, 376 U.S. 483 (1964).

¹² *Harkey v. Abate*, 346 N.W.2d 74 (Mich. Ct. App. 1983).

¹³ *Id.*

¹⁴ For an exception recognizing a cause of action of privacy intrusion in the public sphere, see, Restatement (Second) of Torts, (1977) (Intrusion Upon Seclusion) (Current through July 2002), § 652B cmt. c., see, also, *illus. 7.*; 2. *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 (1995), at 1045-1055 (upholding "public privacy" paradigm and a tortious cause of action).

¹⁵ See, e.g., Restatement (Second) of Torts, § 652B cmt. c. Restatement (Second) of Torts § 652B defines as a tort 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 offensive to a reasonable person." *Id.* Courts in at least twenty-eight states and Federal Government have explicitly or implicitly recognize 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* (5th ed. 1984), at 851 (5th ed. 1984); Reporter's Notes" for the list of practically all states and Federal Government upholding the Restatement (Second) of Torts § 652B Tort of Invasion.

¹⁶ See, also W. Page Keeton et al., *Id.*, § 117, at 855-56; William L. Prosser, *supra* note 9, at 391-92; Andrew Jay McClurg, *supra* note 14, p. 1025; 86 A.L.R.3d 374, *Taking Unauthorized Photographs as Invasion of Privacy* (ed. Phillip E. Hassman), § 2. See, also e.g., *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.*, No. 88-5340, 1988 WL 134497, at *2-3 (6th Cir. Dec. 16, 1988); *International Union v. Garner*, 601 F. Supp. 187, 191 (M.D. Tenn. 1985) (mem.).

¹⁷ W. Page Keeton et al., *supra* note 15, at 855 & n.68; 86 A.L.R.3d 374, *id.*, § 2.

THE CASE OF ON-LINE TERRITORIAL PRIVACY

So far, the territorial facet of privacy has not been adequately applied to privacy in cyberspace since cyberspace is not a physical space and was poorly analogized to one.²⁰ Instead, only a vision of information privacy or data protection has been proffered, as represented in the privacy guidelines issued by the Organization for Economic Cooperation and Development in 1980. These guidelines also outline a set of Fair Information Practices (FIPs) based on eight principles:²¹ collection limitation, data quality, purpose specification, use limitation, transparency of information collection practices, security of stored data, individual participation, and accountability.²² Strictly adhering to the category information privacy, Congress also passed the Electronic Communications Privacy Act (ECPA) of 1986²³ updating the Wiretap Act of 1968.²⁴ Specifically, it expanded the coverage of the Wiretap Act by adding information or database privacy protection through Title 1,²⁵ addressing the unauthorized interception of computer databases or electronic communications²⁶ while “in transit”, and Title 2,²⁷ addressing the unauthorized acquisition of electronic communications while “in storage”.²⁸ Overall, with 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 communications from unauthorized interception, use and disclosure in all private networks, such as in cyberspace.²⁹ In cyberspace, currently,

¹⁸ See, e.g., *Granger v. Klein*, 197 F. Supp. 2d 851 (E.D. Mich. 2002) (Publication in high school yearbook of photograph showing student urinating with his genitalia visible did not constitute intrusion into seclusion, under Michigan law, by school's principal, assistant principal, and 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), *Id.*

¹⁹ W. Page Keeton et al., *supra* note 15, at 855 & n.68; 86 A.L.R.3d 374, *supra* note 16, § 2.

²⁰ See, discussion at Part II.A.1-2, herein.

²¹ See U.S. Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace* (2000) [Hereinafter, 'FTC, Privacy Online'].

²² See Organization for Economic Co-Operation and Development, *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> (last visited Feb. 28, 2004) [Hereinafter, 'OECD Guidelines']. The FIPs have never been fully incorporated into U.S. law. For general discussion, see, Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 *Berkeley Tech. L.J.* 771, 773-81 (1999) [Hereinafter, 'Reidenberg, Restoring Americans' Privacy']; Julie E. Cohen, *DRM and privacy*, 18 *Berkeley Tech. & L.J.* 575.

²³ The Electronic Communications Privacy Act (ECPA), S. Rep. No. 99-541. 99th Cong. 2d Sess. (1986) at 2, reprinted in 1986 U.S.C.C.A.N. 3555 (1986) (ECPA S. Rep.) and codified at 18 U.S.C §§ 2510-2541 (1988) [Hereinafter, 'Senate Report on ECPA'], citing *United States v. New York Tel. Co.* 434 U.S. 159, 167, 98 S.Ct. 364 (1977).

²⁴ 18 U.S.C. §§ 2510-21 and 2701-10

²⁵ *Id.*, §§ 2510-2521 (1988).

²⁶ Electronic communications 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. 18 U.S.C. § 2510(12) (1988), *Id.*

²⁷ *Id.*

²⁸ Electronic storage includes computer random access memory, magnetic tapes, disks, magnetic and optical media, etc. 18 U.S.C. §§ 2701-2710 (1988), *Id.*

²⁹ ECPA expanded the coverage of the Wiretap Act from public common carriers to all private networks, in so doing including all intracompany communications in the protections of wire communications provided by the ECPA. Senate Report on ECPA, at 3. Interception of communications made outside

THE CASE OF ON-LINE TERRITORIAL PRIVACY

there are two basic ways to collect such personal information. The first is by directly collecting information from users (“registration” and “transactional” data).³⁰ Registration data is collected by those websites that request users to log in order to access parts of the website. Transactional data is gleaned by websites engaging in business with users, such as selling merchandise or services.³¹ Second, indirectly, by surreptitiously tracking the way people navigate through the Internet (“clickstream” data), it enables the website to calculate how many times it has been visited and what parts are the most popular.³²

Database protection against such forms of information collection, but particularly registration data that is collected upon initial entry to databases, is arguably an overly generalized and thus over inclusive privacy category.³³ It implicitly includes both possible public and private on-line locales, while overly protecting the former.³⁴ Cyberspace’s experience fails to follow the more multi-dimensional real world’s experience in protecting privacy. In the latter, territorial privacy can be upheld in private locales that are publicly owned,³⁵ such as public telephone booth,³⁶ women employees’ public restrooms owned by their employer³⁷ or a public restroom in a skating rink.³⁸ In cyberspace, however, based on an information privacy category analysis, the type of *ownership* over communication systems, namely private, public or governmental is still the principal criterion in defining a privacy policy for cyberspace as a whole. Thus, without territorial differentiation, privacy protection can be either under- or over-inclusive, for example, in private locales that are publicly owned. In the case of public systems offering electronic communications services to the public, such as AOL, CompuServe, Microsoft Network, and ISPs, in their meaning at the ECPA - the operators of public systems may not disclose the contents of any message, containing identifiable or non-identifiable information. That is, unless an authorized agency produces a court

the United States, however, is not within the scope of ECPA, while U.S. interstate communications “affecting interstate or foreign commerce” are included. 18 U.S.C. § 2510(1) (1988), *Id.*

³⁰ Daniel J. Solove, Privacy and power: Computer databases and metaphors for information privacy, 53 Stan. L. Rev. 1393, at 1411 [Hereinafter, ‘Solove, Privacy and Power’].

³¹ *Id.*

³² *Id.*

³³ Definitions of database or equivalent terms in proposed U.S. legislation, such as the Consumer and Investor Access Bill, have been a little more detailed. See, H.R. 1858 §101(1). See, also, Jacqueline Lipton, Balancing private rights and public reconceptualizing property in databases, Berkeley Tech. Law J. 773 (2003).

³⁴ ECPA differentiates between public and private communication systems solely by type of ownership. It does so for the category of information privacy. Thus, while section 2702(a) in ECPA prohibits the operating owners of public voicemail, email, and other electronic communications systems from disclosing the contents of messages in storage, operators of privately owned corporate systems usually are not restricted by the same prohibitions. See, e.g., *Flanagan v. Epson America, Inc.*; Slip Op. No. BC007036, Ruling on Demurrer and Motion to Strike of Defendant Epson America, Inc. (Cal. Super. Ct., Los Angeles Cty., Jan. 4, 1991). This distinction in ownerships is meant to defend employer’s rights to access their employees’ information in privately owned internal email and voicemail systems. See, e.g., Sharon K. Black, *Telecommunications Law in the Internet Age* (Academic Press 2002), p. 314.

³⁵ Julie E. Cohen, *supra* note 22, at 578-579.

³⁶ *Katz v. United States*, *supra* note 41, *Id.*

³⁷ *Benitez v. KFC Nat'l Mgmt. Co.*, 714 N.E.2d 1002 (Ill. App. Ct. 1999).

³⁸ *Harkey v. Abate*, 346 N.W.2d 74 (Mich. Ct. App. 1983).

THE CASE OF ON-LINE TERRITORIAL PRIVACY

order to review the message;³⁹ regardless of whether it has been collected in what would otherwise be regarded an on-line public locale, where such collection would then have been authorized. Thus, customers of companies providing electronic communication services to the public, through public systems such as voicemail and email, have an over-inclusively strong expectation that all their communications, direct and indirect, are private and that the service provider will simply transmit and store the message until it is retrieved and deleted by the customer, as wrongly analogized with the category of privacy of communications in the analog telephone communication systems; or even digital communications systems. The tendency of data collectors and users alike should, instead, be to relocate so to maximize the congruence between their preferences and particular territorial locales.⁴⁰ Consequently, as Tiebout's well-known theorem all-purposely predicts, the further allocation of legal rights to different types of territorial locales, predominantly private and public, would exercise strong effects upon the heterogeneity of data collection practices, justifying the geographical variation of on-line privacy rules altogether.⁴¹

The legal rule in public locales should then balance privacy protection with protecting 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. That is, either directly (collecting registration and transactional data) or indirectly (collecting clickstream data) by websites. 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.⁴² On balance, adaptation of ECPA's "in storage" definition in Title II, primarily, to territorial privacy would then enhance the legitimate protection given against information collection in on-line private locales.

Moreover, database protection falls short of applying information privacy whenever an otherwise potential locale would include multiple privately protected databases. Identifying such databases as private or public locales may then avoid over fragmentation of regulative realms.⁴³ Indeed, for the real world, courts have rejected cases involving territorial intrusion whenever the category of privacy that would likely be infringed was done in databases and would therefore belong to the category of information or database privacy, such as, while rejecting obtaining a person's unlisted phone number,⁴⁴ the selling

³⁹ 18 U.S.C. § 2702(a). See also, *Deal v. Spears*, 780 F. Supp. 618 (W.D. Ark. 1991), *aff'd*, 980 F.2d 1153 (8th Cir. 1992) (employer recording of personal phone calls served no legitimate purpose). See, generally, Sharon K. Black, *supra* note 34, at 313.

⁴⁰ C. M. Tiebout, *The pure theory of local expenditure*, *Journal of political economy* 64 (October) (1956), pp. 416-424.

⁴¹ *Id.*

⁴² See, e.g., Solove, *Privacy and Power*, *supra* note 30, at 1433. See, also, discussion in Part III.B.2, *infra*.

⁴³ See, e.g., Julie E. Cohen, *supra* note 22, at 592 (applying this observation to computers in the physical space, which sit at the center of such privacy zones, regardless of where in physical space it happens to be located).

⁴⁴ *Seaphus v. Lilly*, 691 F. Supp. 127, 132 (N.D. Ill. 1988).

THE CASE OF ON-LINE TERRITORIAL PRIVACY

subscription lists to direct mail companies,⁴⁵ or the collecting and disclosing an individual's past insurance history.⁴⁶

In analogy to the real world, the suggested adaptation of territorial privacy to cyberspace based on the tort of intrusion upon seclusion will overcome these anomalies, as the paradigm of private and public locales would stop resting primarily upon the circumstance of ownership, overcoming the proprietary-based analysis of trespass to chattels.⁴⁷ In fact, territorial privacy and private and public locales, more specifically, could coexist on the Internet, just as they do in the physical world.⁴⁸ Courts may then be required to differentiate and identify public locales and then fence them out 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 too wide, privacy legal rule has been adopted. In continuation to previous jurisprudential developments, privacy should continue to be revalued instrumentally.⁴⁹ Ultimately, a legal fiction of on-line locales should now be constructed for cyberspace's overall privacy policy.⁵⁰ For such legal fiction to be effectively applicable and harmonious with privacy protection at large, a comprehensive boundary framework for cyberspace has to first be agreed upon, as explained in Parts II-VI, in the following order.

⁴⁵ Shibley v. Time, Inc., 341 N.E.2d 337, 339 (Ohio Ct. App. 1975).

⁴⁶ Tureen v. Equifax, Inc., 571 F.2d 411, 416 (8th Cir. 1978).

⁴⁷ 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. Restatement (Second) of Torts § 217(b) (1965). See, also, Curtis J. Berger, Pruneyard Revisited: Political Activity on Private Lands, *Id.*, at 655 (similarly arguing for the real world). Further on, 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 (1996), at 61.

⁴⁸ 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. 1609, 1657 (1999), at 1664 (adding to the public and private also the quasi-public locale), at 1667. Notwithstanding the importance of the latter category, and in compliance with the tort of intrusion jurisprudence, I will ignore the latter category. See, also, discussion, herein.

⁴⁹ See, also, Solove, Conceptualizing Privacy, *supra* note 9, at 1144-1145; Julie C. Inness, *supra* note 1, at 95. One example is the Court's 1928 decision in *Olmstead v. United States* 277 U.S. 438 (1928) epitomizes 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. Only in 1967, overruling *Olmstead* did the *Katz v. United States* 389 U.S. 347 (1967) hold construct that wiretapping does not necessitate physical trespass. See, also, Carl Shapiro & Hal R. Varian, U.S. Government Information Policy 45 (July 30, 1997) <<http://www.sims.berkeley.edu/~hal/Papers/policy/policy.html#SECTION00081000000000000000>> (Section on Privacy).

⁵⁰ See generally, also, Andrew L. Shapiro, Street Corners in Cyberspace, *The Nation*, July 3, 1995 (in justification of the 1st 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 (Winter 1998), at 3 (same). See, also discussion, herein.

THE CASE OF ON-LINE TERRITORIAL PRIVACY

Part II provides with an overview of the two competing boundary approaches for cyberspace. Arguably, thus far, cyberspace is still left without a comprehensive boundary approach and Courts or legislators have not yet been successful in collectively adopting one. In theory, however, cyberspace boundary discourse is, nevertheless, present, and has thus far only given rise to two conflicting approaches, referred to herein as the ‘globalist’ and the ‘anti-globalist,’ while largely ignoring the more sensible legal alternative – one based on a ‘localist’ boundary approach, which will be critically assessed in this part.

The first, therefore, is the globalist boundary theory approach. It is a rather optimistic technologically-oriented analysis, which suggests that cyberspace is bound to be zoned similarly to the real world, although separate on-line spatiality does not exist, according to Lessig or Shapiro, most notably; or that spatiality exists separately from the real world and might allow some degree of zoning, according to Johnson and Post. In both ways, spatiality is seen merely as a technological constraint that would override any legal definition of spatiality. In essence, both are looking for a technological solution and, in fact, underestimate the role of law in erecting boundaries in cyberspace. Both, therefore, 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 cyberspace; as Cyberspace is not a real ‘place’, but instead a medium and tangible objects do not exist “there”.⁵¹

Geared with the motivation to find and legalize their underlying scientific truths, both the globalist and anti-globalist approaches share a tendency to over-scientize the law in those instances when science and law interact, as then can be applied through the case of on-line territorial privacy protection. Arguably, both approaches do not seem to have appropriately dealt with challenge 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, such as the one suggested for the formalization of on-line spatiality, should then, in fact, be a tentative scientific truth transformed from mere scientific truths, backed by legal values, to an inclusive legal truth by courts or other regulating institutions.

As would be reminded, Anglo-American jurisprudence has a long record of viewing factual or scientific truth as only one parameter in establishing legal truth. The factual or scientific validity of spatial or non-physical boundaries, therefore, should not inherently serve as a binding constraint on a possible legal formation of on-line locales. In continuation, areal or local differentiation should now replace the homogenous spatial organization as the major conceptual focus of cyberspace’s globalist boundary theory.

⁵¹ See, e.g., Dan Hunter, *Cyberspace as place and the tragedy of the digital anticommons*, 91 Cal. L. Rev. 439 (2003), at 472; Mark A. Lemley, *Place and Cyberspace*, 91 Cal. L. Rev. 521 (2003), at 523; Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U. Chi. Legal F. 217, at 217; Maureen A. O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 Berkeley Tech. L.J. 561 (2001), at 567 [Hereinafter, ‘O'Rourke, Property Rights’].

THE CASE OF ON-LINE TERRITORIAL PRIVACY

Consequently, the allocation of legal rights to different types of locales, predominantly private and public, may then exercise strong effects upon the heterogeneity of data collection practices, justifying the geographical variation of on-line privacy rules altogether.

Part III, consequently, upholds that law may indeed construct a legal fiction of on-line locales. Seen through the prism of the cumulative characteristics of legal fictions, this chapter confronts both globalist and anti-globalist boundary rationales, in support of the comprehensive theoretical structure of localist boundary application to 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 deduces several policy rationales concerning the prospect of integrating territorial privacy in cyberspace. It concludes by suggesting that notwithstanding the category of information privacy protection, territorial privacy upon cyberspace's private and public locales, more specifically, could coexist on the Internet, similarly to the physical world. Courts may then be required to differentiate and identify public locales and then fence them out from private ones.

II.
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’.⁵² 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.⁵³ In this sense, space is the conceptualization of the imagined physical relationships, which gives meaning to society.⁵⁴ Locale, on the other hand, is the distinct space that encompasses both the idea and the actuality of where things are.⁵⁵ Referring to the nested hierarchy of bounded spaces of differing size, such as the local, regional, national and global, is a familiar and taken-for-granted concept of political geographers and political analysts.⁵⁶ Thus, numerous scholars have employed a framework that employs three scales of analysis – international or global, national or state level, and an intra-national, usually an urban metropolitan scale.⁵⁷ They are relatively closed and self-sufficient systems.⁵⁸

Incorporated also into the real world’s legal discourse, two main competing interpretive border theories, thus far, have developed: A globalist and a localist, each, as will be explained, insufficiently attentive to the values represented by the other.⁵⁹ They pivot around the basic unit of the state- hence the international, national and intra-national

⁵² See, e.g., Daniel A. Farber, *Stretching The Margins: The Geographic Nexus in Environmental Law*, *Stan. L. Rev.* 1247 (1996), at 1247, 1273-1275 (in application to international environmental law); Christopher D. Stone, *Locale and Legitimacy in International Environmental Law*, *Stan. L. Rev.* 1279 (1996) (same).

⁵³ For matters of convenience, the terms ‘locale’ and ‘location’ would be used correspondingly. Edward W. Soja, *A paradigm for the geographical analysis of political systems* (1974), 43-71, In *Locational approaches to power and conflict*, Kevin R. Cox, David Reynolds & Stein Rekkas (Eds.), at 53 [Hereinafter, ‘Soja, A paradigm’]; R.J. Johnson, *spatial structures* (Mathuen: London, 1973), p. 14; Hence Short, *An introduction to political geography* (Routledge & Kegan Paul: London, 1982) 1; David Delaney & Helga Leitner, *The political construction of scale*, *Political Geography*, Vol. 16 No. 2, 93 (1997), at 93.

⁵⁴ M. Keith & S. Pile, (eds.), *Place and Politics of identity* (London Routledge, 1993); A. Gupta, *Blurred boundaries: The discourse of corruption, The culture of politics, and the imagined state*, *American Ethnologist* vol. 22, no. 2 (1992), at 375-402.

⁵⁵ *Id.*, at 375-402.

⁵⁶ David Delaney & Helga Leitner, *supra* note 45, at 93.

⁵⁷ See, e.g., Peter Tylor, *Political geography: world-economy, nation-state and locality* (Longman Scientific & technical, 1993), p. 43.

⁵⁸ R.J. Johnson, *supra* note 45, at 14.

⁵⁹ Hastings Donnan & Thomas M. Wilson, *Borders: Frontiers of Identity, Nation and State* (Berg, 1999), at 9; Daniel A. Farber, *supra* note 44, at 1247, 1248, 1270-1271 (investigating the conflict between localist and global perspectives in environmental law); Edward Soja, *Surveying Law and Borders – Afterward*, *Stan. L. Rev.* 1421 (1996), at 1426 (same) [Hereinafter, ‘Soja, Surveying Law and Borders’]; Soja, *A paradigm*, *supra* note 45, at 53.

THE CASE OF ON-LINE TERRITORIAL PRIVACY

terminology.⁶⁰ The first is a *spatial* analysis, which refers to globalist boundary theory as has been adopted, for instance, in international environmental or even international criminal law. Globalism gives every government an equally legitimate concern with every issue, without offering any line drawing rationale, and, in that sense, attempts to erase geographic discontinuity. The basic idea of globalism is that legal controversies know no territorial boundaries. What happens in one place affects everyone everywhere, and no particular geographic nexus should be required as a basis for legal action.⁶¹ According to the globalist approach, geographical uniformity is not an inevitable feature of a legal rule.⁶²

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.⁶³ At the international level, localism is surely the baseline.⁶⁴ 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.⁶⁵ 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. Arguably, thus far, cyberspace is still left without an applicable boundary approach and Courts or legislators have successfully adopted none. In theory, however, cyberspace boundary discourse is, nevertheless, present, and has thus far only given rise to two conflicting approaches, globalist and anti-globalist, while largely ignoring the more sensible legal alternative – one based on a localist boundary approach, which will be critically assessed herein.

Thus far, 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. It's rather optimistic, technologically-oriented analysis suggests that cyberspace is bound to be zoned similarly to the real world, although separate on-line spatiality does not exist, according to scholars like Lessig or Shapiro, most notably, or that spatiality exists separately and might allow some degree of zoning, according to Johnson and Post. 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. Law is a sideshow. Thus, this technological primacy is more than a

⁶⁰ See, e.g., Peter Tylor, *supra* note 49, at 44.

⁶¹ See, Daniel A. Farber, *supra* note 44, at 1272.

⁶² See, Gerald L. Neuman, *Anomalous Zones*, *Stan. L. Rev.* 1197 (1996), at 1201.

⁶³ Daniel A. Farber, *supra* note 44, at 1270; Soja, *A paradigm*, *supra* note 45, at 53.

⁶⁴ Daniel A. Farber, *Id.*, at 1270; Soja, *A paradigm*, *Id.*, at 53.

⁶⁵ *Id.*, Daniel A. Farber, at 1270.

THE CASE OF ON-LINE TERRITORIAL PRIVACY

difference in efficiency.⁶⁶ In essence, both are looking for a technological solution, which arguably underestimate the role of law. Both, overall, 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 none can be put in its place. As will be briefly described herein, both the globalist and the anti-globalist approaches alike do not seem to appropriately have dealt with challenge to the underlying 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.

A. *Globalist boundary theory: Johnson & Post and Lessig*

Until the digital era, there has been 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".⁶⁷ Nowadays, cyberspace is dealing with a genuine fencing challenge with 'law space', 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.⁶⁸ 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 and, in some cases, 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 seemed to have generally followed this technocentric line of argumentation. That choice was ultimately encapsulated in the constituting case of *Reno v. ACLU*,⁶⁹ where the Court concluded that the Internet was deserving of full First Amendment protection, not the lesser protection afforded to broadcast media. In so doing, the Court considered how well each metaphor actually applied cyberspace. The court concluded that cyberspace allowed the construction of barriers and their use to screen for identity, making cyberspace more like the physical world and, consequently, more amenable to zoning laws.⁷⁰ Justice O'Connor's opinion makes that very controversial assumption, observing "[c]yberspace undeniably reflects

⁶⁶ L. Lessig, *The Constitution of Code: Limitations on Choice—Based Critiques of Cyberspace Regulation*, 181 (1997), at 182; L. Lessig, *Code and Other Laws of Cyberspace*, (basic books, 1999), at 130 [Hereinafter, 'Lessig, Code and Other Laws'].

⁶⁷ David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 *Stan. L. Rev.* 1367 (1996), at 1368 [Hereinafter, 'Johnson & Post'].

⁶⁸ Jonathan J. Rusch, *Cyberspace and the "Devil's Hatband,"* 24 *Seattle U. L. Rev.* 577, 591-92 (2000), at 585.

⁶⁹ See, 521 U.S. 844, 117 S. Ct. 2329 (1997).

⁷⁰ *Id.*, at 2354.

THE CASE OF ON-LINE TERRITORIAL PRIVACY

some form of geography; chat rooms and Web sites, for example, exist at fixed 'locations' on the Internet".⁷¹

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 real 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 itself popularity among the academic community. The works of Lawrence Lessig, Andrew Shapiro, Trotter Hardy, and others are perhaps those that most paved the way in that direction. In compliance with the Court's continuity choice, unlike Johnson and Post, who argue for a separation between real space law and Cyberspace law, Lessig, most notably, does not believe that it can be sustained or that it should be.⁷²

Putting much faith in technology at the expense of a weakened legal solution, Lessig promises us "what is missing in discourse about Cyberspace and its regulation is a richer understanding of the range of architectures that are possible".⁷³ The architecture of Cyberspace, we are told, will in principle allow for perfect zoning--a way to perfectly exclude those who would cross boundaries.⁷⁴ Advances in technology, not law, we are told, will make zoning the Internet feasible in the future.⁷⁵

Overall, Lessig and Hardy and others agree that zoning will replace the present wilderness of Cyberspace, implicitly adhering to an inclusive globalist boundary approach in cyberspace, 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.⁷⁶ In further recognition of a spatial approach to cyberspace, it is, then, probably the case that both the

⁷¹ See, 117 S. Ct. at 2353 (O'Connor, J., concurring in the judgment in part and dissenting in part). For opposing opinions in few lower instances, see, e.g., *American Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 168-69 (S.D.N.Y. 1997) ("[G]eography, however, is a virtually meaningless construct on the Internet."); *Digital Equip. Corp. v. Altavista Tech., Inc.*, 960 F. Supp. 456, 462-63 (D. Ma. 1997).

⁷² Lawrence Lessig, *The zones of cyberspace*, *Stan. L. Rev.* 1403 (1996), at 1403 [Hereinafter, Lessig, *Zones of cyberspace*']; Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 *Harvard Law Review* 501 (1999), at 3, 55; Andrew L. Shapiro, *The Disappearance of Cyberspace and the Rise of Code*, 8 *Seton Hall Const. L.J.* 703 (1998), at 704, 714-715 [Hereinafter, 'Shapiro, *The Disappearance*'] and Fn. 29 & additional sources there. See, also, Soja, *Surveying Law and Borders*, *Supra* note 51, at 1427. For earlier observations, see also, M. Ethan Katsh, *Rights, Camera, Action: Cyberspatial Settings and the First Amendment*, 104 *Yale L.J.* 1681 (1995), referring to Joshua Meyrowitz, *No sense of place: The impact of electronic media on social behavior* (1985), at 38 ([P]hysical settings and media "settings" are part of a continuum rather than a dichotomy), at 1686.

⁷³ Lawrence Lessig, *The Architecture of Privacy*, 1 *Vand. J. Ent. L. & Prac.* 56 (1999), at 60, 64.

⁷⁴ Lessig, *Zones of cyberspace*, *supra* note 64, at 1409.

⁷⁵ Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 *Emory L.J.* 869, (1996), at 886-901.

⁷⁶ Lessig, *Zones of cyberspace*, *supra* note 64, at 1409.

THE CASE OF ON-LINE TERRITORIAL PRIVACY

cost of drawing borders--identifying digital information as one's own--and the cost of monitoring border trespasses--detecting unauthorized copying or alterations--seem to be no higher in Cyberspace than they are for real property.⁷⁷ Such costs may even be lower in Cyberspace thanks to recent technological developments.⁷⁸

In opposition to Lessig's view regarding a continuous physical-virtual spatiality lays a competing globalist boundary approach, which suggests that specialty in cyberspace, is in fact, separate from that of the physical world. This view, as well, upholds a strict technologically centered approach, while suggesting that spatiality is mostly a technological concern.⁷⁹

The leaders of this alternative libertarian orthodoxy are David Post and David Johnson.⁸⁰ Their major explicit globalist premise, therefore, is that Cyberspace is a space or has the characteristics of a space, in disconnection from physical space.⁸¹ As they suggest, many of the jurisdictional and substantive quandaries raised by border-crossing electronic communications could be resolved by one simple principle: conceiving of Cyberspace as a distinct space for purposes of legal analysis by recognizing a legally significant border between Cyberspace and the physical world.⁸² On a normative level, their argument then follows to argue against the adaptation of "geographic legal space" to "cyber space or spaces". Traditional legal reasoning, we are told, 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.⁸³ Thus, any insistence on

⁷⁷ Trotter Hardy, *supra* note 43, at 259.

⁷⁸ *Id.*

⁷⁹ See, e.g., Lawrence Lessig & Paul Resnick, Zoning Speech on the Internet: A Legal and Technical Model, 98 Mich. L. Rev. 395 (1999), at 396; Lawrence Lessig, The Death of Cyberspace, Wash. & Lee L. Rev. 337 (2000), at 344 [Hereinafter, 'Lessig, The Death of Cyberspace'].

⁸⁰ Johnson & Post, *supra* note 59, 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, primarily, John Perry Barlow, Is There a There in Cyberspace?, at: <www.eff.org/Publications/John_Perry_Barlow/HTML/utne_community.html> (last visited October 1, 2003); see also Esther Dyson et al., Cyberspace and the American Dream: A Magna Carta for the Knowledge Age (Aug. 22, 1994), at <www.pff.org/position_old.html> ; Mitchell Kapor & John Perry Barlow, Across the Electronic Frontier, July 10, 1990 (July 10, 1990), available at <www.eff.org/pub/Publications/John_Perry_Barlow/HTML/eff.html>, reprinted in Robert B. Gelman & Stanton McCandlish, Protecting Yourself Online: The Definitive Resource on Safety, Freedom, and Privacy in Cyberspace 14 (1998).

⁸¹ Johnson & Post, *supra* note 59, at 1379, 1381.

⁸² *Id.*, p. 1378.

⁸³ *Id.*, 1370-72. See, also, Dan L. Burk, Federalism in Cyberspace, 28 Conn. L. R. 1095 (1996), at 1098-99 [Hereinafter, 'Burk, Federalism']; 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*, Emory L. J. 911 (1996), at 84, 85-87 [Hereinafter, 'Reidenberg, Governing Networks']; See, 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").

THE CASE OF ON-LINE TERRITORIAL PRIVACY

"reducing" all on-line transactions to a legal analysis based in geographic terms presents, in effect, a new "mind-body" problem on a global scale.⁸⁴

As a legal matter, leading an original globalist border theory approach to cyberspace, they treat Cyberspace as a separate "space" to which the application of distinct sets of laws should come naturally.⁸⁵ Therefore, we must either refrain from applying these ineffective real-space laws to Cyberspace, or devise new laws or modes of regulation that can effectively regulate Cyberspace. In reaching their result they argue why 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 on line.⁸⁶ 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.⁸⁷

Using this new approach, they suggest, we would no longer ask the unanswerable question "where" in the geographical world a Net-based transaction occurred.⁸⁸ In conclusion, Johnson and Post argue that the power to control activity in Cyberspace has only the most tenuous connections to physical locales.⁸⁹ Upholding a typical globalist boundary approach in Cyberspace, they argue, physical borders no longer function as signposts informing individuals of the obligations assumed by entering into a new, legally significant, space.⁹⁰ Individuals are unaware of the existence of those borders as they move through virtual space.⁹¹

Interestingly enough, these two globalist boundary approaches to cyberspace are mostly compared for what they disagree about; that is, whether specialty in cyberspace is separate than that of the physical world. At the same time, it is important to mention that both views also seem to share similar globalist spatial proposition. Both, in fact, 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 positively concur that as much as zoning can serve us to uphold on-line locality, strict 'gateway' technology zoning is capable to provide a comprehensive boundary theory, that is, clearly without the need or ability to construct of legal solutions, such as the legal fiction of on-line locales.

As would be argued later on, a preferred localist boundary theory and practice in cyberspace, may in fact allow us to avoid the technological challenge of zoning cyberspace with totality – the problematic creation of an inherent continuous space within

⁸⁴ Johnson & Post, at 1378.

⁸⁵ *Id.*, at 1379; David Johnson & David Post, And How Shall the Net Be Governed? A Meditation on the Relative Virtues of Decentralized, Emergent Law, in *Coordinating the Internet* 62 (Brian Kahin & James Keller, eds., 1997); Post, *Governing Cyberspace*, at 159.

⁸⁶ See, e.g., Post & Johnson, *Chaos Prevailin*, at 1059.

⁸⁷ Johnson & Post, at 1379, 1381.

⁸⁸ *Id.*

⁸⁹ *Id.*, at 1371.

⁹⁰ *Id.*, at 1375.

⁹¹ *Id.*

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 technocentric 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. Secondly, it also falls short of adhering to a legal zoning solution in the case technology fails to, while wrongly concluding that because physical borders are not applicable, the only 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.⁹² Accordingly, there is a need not only for understandings of what legal rules govern but also how they relate to each other.⁹³ In disagreement with these globalist boundary approaches, this study later on 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 lays an alternative anti-boundary theory one. Like its counter version, it 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 "[I]t is wishful thinking to assume that geographic indeterminacy will prevail and that the Internet is pure information".⁹⁴ Accordingly, Courts can and should take the differences between cyberspace and the real world into account,⁹⁵ as this notion can have a profound consequence for legal analysis.⁹⁶ The recognition that the Internet is not just like the real world, and that the ways in which it is different may matter to the outcome of cases, is critical.⁹⁷ Consequently, strict factual or scientific truth holders, such as Hunter and Lemley tell us that because the metaphor is not just like the real world – courts inappropriately use it. Their main message is that Cyberspace is not a real global space, of course, and tangible objects do not exist in locales "there".⁹⁸ Thus, declining the globalist spatial assumption for cyberspace, it suggests that the analogy between the Internet and a physical space and locales is not sustainable.⁹⁹ These views as well,

⁹² See, Maureen A. O'Rourke, *Fencing Cyberspace: Drawing Borders in a Virtual World*, 82 Minn. L. Rev. 609, 641-45 (1998), at 613 [Hereinafter, 'O'Rourke, Fencing Cyberspace']..

⁹³ *Id.*

⁹⁴ See, e.g., Joel R. Reidenberg, *Yahoo and democracy on the Internet*, 42 *Jurimetrics J.* 261 (2002), at 274.

⁹⁵ See Mark Lemley, *supra* note 43, *Id.*; Maureen A. O'Rourke, *supra* note 43, at 561.

⁹⁶ See, Maureen A. O'Rourke, *Id.*, at 592 and Fn. 62, referring to Robert G. Sachs, *the Physics of Time Reversal I* (1987).

⁹⁷ Mark Lemley, *supra* note 43, *Id.*

⁹⁸ See, Dan Hunter, *supra* note 43, at 472; Mark A. Lemley, *supra* note 43, at 523; Trotter Hardy, *supra* note 43, at 217; Maureen A. O'Rourke, *supra* note 43, at 567.

⁹⁹ See, Mark Lemley, *supra* note 43, *Id.*; Josh A. Goldfoot, *Antitrust Implications of Internet Administration*, 84 *Va. L. Rev.* 909, 920 (1998).

THE CASE OF ON-LINE TERRITORIAL PRIVACY

nevertheless, seem to undermine the importance of the legal constraint in the search for comprehensive and sustainable boundary solutions. According to this version of the globalist boundary discourse, factual or scientific truths, in fact, stand for a skeptical view of the technological constraint.

Both the globalist and the anti-globalist approaches, in their way, seem to uphold an absolute view of the question of on-line spatiality, while adhering to an “all-or-nothing” regulative view regarding the existence of a globalist perception of an on-line space. From a legal perspective, this technocentric factual or scientific truth should instead be only one parameter in establishing a legal truth and is but the handmaiden of the legal system.¹⁰⁰ In opposition to these views, arguably, legal reasoning must now expand existing jurisdictional rules into workable legal doctrine also in cyberspace, as made possible through the prism of the localist boundary approach.

¹⁰⁰ 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.). See, also discussion in Part III, *infra*.

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

A. *Overview*

Legal truth, suggested here for the formalization of on-line spatiality, is in fact a tentative scientific truth, backed by legal values, to an inclusive legal truth constructed by courts or other regulating institutions. Fuller frames a legal fiction as a false statement recognized as having utility,¹⁰¹ or a statement propounded with a complete or partial consciousness of its falsity.¹⁰² This part shows that both settings, in fact, entail a more pragmatic framework to formalizing on-line locales, whenever localist boundary theory is applied. In continuation, a legal fiction is then constructed through a three criteria classification scheme. First, a legal fiction has to be based on an inference justified by common experience in 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. Lastly, a legal fiction has to be phrased in realistic terms. A final construction of a legal fiction of on-line locales based in its meaning in localist boundary theory, would then comply with the line of argument suggested herein, which upholds that eventually positive law and particularly territorial privacy, can and should be applied to all of Cyberspace effectively. Whenever the legal fiction of on-line locale can provide, cyberspace should not be in any way special or immune from legal reach, such as in the case of territorial privacy law jurisprudence.

B. *The Epistemological framework:*

1. *Recognition of Utility, or*

A legal fiction can be a false statement recognized as having utility.¹⁰³ Such legal fictions would then be constructed upon their functionality.¹⁰⁴ That requirement is also met by localist boundary theory, suggesting that there should be a local center that would provide 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

¹⁰¹ Lon L. Fuller, *Legal Fictions* (1967), at 9.

¹⁰² *Id.*

¹⁰³ L. Fuller, *Supra* note 131, at 9. 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 R.E. Kasperson & J.V. Minghi (eds.), *The structure of political geography* (Chicago: Aldine, 1969), at 146; R.E. Kasperson & J.V. Minghi (eds.), *The structure of political geography*, 'Structure: Introduction' (Chicago: Aldine, 1969), at 77-78.

¹⁰⁴ Consequently, after their useful function had ended, legal fictions should and could be readily removed. See, Aviam Soifer, *supra* note 161, at 875 and Fn 11 & accompanying text.

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. Lastly, the construction of on-line locales upon their functionality would need to be based on the alternative certainty that formalizing legal locales on-line indeed is feasible.

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 truisms - nevertheless seems to be based on a largely accepted deformations of cyberspace's architecture, in comparison to that of the real world's. This distortion is largely threefold, referring 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 real world in comparison to cyberspace. In the real world the public/private distinction arose out of a double movement in modern political and legal thought.¹⁰⁵ 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.¹⁰⁶ On the other hand, in reaction to the claims of monarchs, and later parliaments, to the unrestrained power to make law, a countervailing effort to stake out distinctively *private* locales free from the encroaching power of the state developed.¹⁰⁷ 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.¹⁰⁸ By 1934, the areas that people considered the most valuable for mines, agriculture, forestry, water development, and other uses had already been

¹⁰⁵ For the Anglo-American origins of the distinction, see, Morton J. Horwitz, *The History of the Public/Private Distinction*, U. Pa. L. Rev. 1423 (1982), at 1423 and Fn.1 referring to D. Hanson, *From Kingdom to Commonwealth* 1-19 (1970).

For the North American experience, see the works of, Gerald E. Frug, *The City as a Legal Concept*, 93 Harv. L. Rev. 1059 (1980). Frug works almost exclusively from secondary sources; 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); Morton J. Horwitz, *supra* note 172 (a thumbnail sketch of the history of the distinction).

¹⁰⁶ Morton J. Horwitz, *Id.*, at 1423.

¹⁰⁷ *Id.*, 1423 and Fn. 2, referring to historical sources to support that observation.

¹⁰⁸ *Id.*, at 1423.

THE CASE OF ON-LINE TERRITORIAL PRIVACY

appropriated.¹⁰⁹ What were left behind (to what later became the vastly overextended 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.¹¹⁰ Later on, moreover, in the early years of the conservative Burger Court, the private sphere was further narrowed.¹¹¹ In the real world, thus far, an interventionist theory to limit the private sphere has not prevailed and the public sphere continued to serve as the default rule.¹¹² 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.¹¹³

In cyberspace the opposing trend unmistakably has prevailed. While the real 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 web sites. As pictorially put by Maureen Ryan, cyberspace has 'no town halls, no granges, no public squares, no downtown churches or galleries or schools'.¹¹⁴ Thus neither public locales nor balanced territorial privacy policy have so far 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,¹¹⁵ where information such as the Internet's is a major source of wealth aggregation, what has been the original exception seems to have become the norm.¹¹⁶ As Carol Rose points out, this 'propertization' trend did not occur in a vacuum, but rather came directly at the expense

¹⁰⁹ See, Carol Rose, *Romans, Roads, and Romantic Creators: Traditions of Public Property in the Information Age*, 66 *Law & Contemp. Probs.* 89, at 5, referring also to George Cameron Coggins, Charles F. Wilkinson, and John D. Leshy, *Federal Public Land and Resources Law* (4th ed. 2001), at 133-34.

¹¹⁰ *Id.*, George Cameron Coggins, at 133-34, 139, 142-43.

¹¹¹ See, e.g., Donald R.C. Pongrace, *Stereotypification of the fourth amendment's public/private distinction: An opportunity for clarity*, 34 *Am. U. L. Rev.* 1191 (describing a process of narrowing the private sphere in the years the 80's Burger court), at 1191-1192 and Fn. 6-8 and accompanying text; Commentators use the term 'Burger Court' to signify the conservative majority that currently dominates the United States Supreme Court. See Schwartz, *Fifteen Years of the Burger Court*, 239 *Nation* 262 (1984) (describing Court's conservative trend since Warren Burger started his first term as Chief Justice in 1969).

¹¹² Louis Michael Seidman, *supra* note 157, at 1011 and Fn. 17 & accompanying text. (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, L. Seidman, C. Sunstein & M. Tushnet, *Constitutional Law* 739-41 (1986), at 575-78.

¹¹³ See, Louis Michael Seidman, *supra* note 157, 1010-1011 and Fn. 18 & accompanying text.

¹¹⁴ Maureen Ryan, *Cyberspace as a public space: A public trust paradigm for copyright in a digital world*, 647 *Or. L. Rev.* (2000) and Fn. 249 & accompanying text.

¹¹⁵ On the shift from the industry economy to the present information economy, see, Patricia Mell, *supra* note 112, at 17, referring to Bell, Daniel Bell, *The Coming of the Post-Industrial Society* 47-119 (1973), at 47-119.

¹¹⁶ Lawrence Lessig, *supra* note 66, at 59.

THE CASE OF ON-LINE TERRITORIAL PRIVACY

of what might seem to be 'un-ownable' diffuse resources or *res communes* in the tangible world.¹¹⁷ Left to self-regulatory approaches, sufficient and legally protected public locales arguably will not evolve, and an inner balance between private and public locales and territorial privacy policy more particularly, will not be achieved.¹¹⁸

Second, as opposed to the real 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 real 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, as 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.¹¹⁹ 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. In cyberspace, however, 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 web sites, are not dependently accessible among themselves and for that reason were not seen as inflicting additional transfer cost to neighboring private locales. To conclude, in cyberspace, there is no need for transfer permission between private web sites. Neither is there an inherent technical need to subsidize transfer costs through the construction of public locales as a mean 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. Such is also the prevailing practice in real time "chat rooms",¹²⁰ news groups,¹²¹ and

¹¹⁷ Carol M. Rose, *supra* note 176, at 7; See, also, Paolo Carpiagnano et al., Chatter in the Age of Electronic Reproduction: Talk Television and the "Public Mind," in *The Phantom Public Sphere* 93 (Bruce Robbins ed., 1993), at 96-97, at 93 ((relating this pattern to the more broad influence of mass media).

¹¹⁸ See, particularly, discussion in Part III.C.2, *infra*.

¹¹⁹ Robert C. Ellickson, *supra* note 114, at 1383-1384.

¹²⁰ Chat rooms allow interested individuals to participate in on-line discussions in real time on a myriad of general interest topics by sending and receiving messages via their ISP. See generally *ACLU v. Reno*, *supra* note 61, at 834-36 (surveying common methods of communication on the Internet).

¹²¹ Usenet news groups are a loosely organized collection of distributed bulletin boards, each one dedicated to a particular topic. See generally *ACLU v. Reno*, *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").

remote information retrieval practices such as bulletin-board services and message boards.¹²² 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 governments' technocentric self-regulation approaches enhance these areas to the protected legal status of public locales, nor do they act to reestablish the balance between both types of locales, in favor of the latter. Third, in opposition to the physical world, transaction costs generated by web sites 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 their corrective minimization, 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, which implies that law suffers from an inherent inability to correct this anomaly. That is, as the analogy between the Internet and a physical locale is not particularly strong,¹²³ scientific truism largely upholds that it is wishful thinking to assume that legally made geographic indeterminacy could prevail.¹²⁴ The recognition that the Internet is not just like the real world, and that the ways in which it is different may matter to the outcome of cases, we are told, is critical.¹²⁵ In fact, the United States federal government's privacy policy still encourages the withdrawal of law as a balancing constraint, as seen with the FTC's stance toward online privacy, which emphasizes self-regulation via the adoption of privacy policies.¹²⁶ Arguably, technology alone, thus far, has failed to provide protection comparable to that, which is provided in law.¹²⁷ It is, at least presently, 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.

¹²² See, generally, *ACLU v. Reno*, supra note 61, at 834-36.

¹²³ See, e.g., Mark Lemley, supra note 43, id; Josh A. Goldfoot, supra note 88, at 920 ("At best 'cyberspace' is a convenient term describing a set of communications achieved through the Internet.").

¹²⁴ See, e.g., Reidenberg, *Yahoo and democracy*, supra note 89, at 274; Lawrence Lessig & Paul Resnick, supra note 72, at 396; Lessig, *The Death of Cyberspace*, at 344; Johnson & Post, at 1379; Post & Johnson, *Chaos Prevailing*, supra note 73, *Id*; Post, *Governing Cyberspace*, at 161.

¹²⁵ See, Maureen A. O'Rourke, supra note 43, at 592 and Fn. 62, referring to Robert G. Sachs, *the Physics of Time Reversal 1* (1987).

¹²⁶ 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 (1995), at 508-11 [Hereinafter, 'Reidenberg, Setting Standards'].

¹²⁷ Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, *Stan. Tech. L. Rev.* 1 (2001), at 79; See, Joel Reidenberg, Jennifer Barrett, Evan Hendricks, Solveig Singleton & David Sobel, 11 *Fordham Intell. Prop. Media & Ent. L.J.* 59, at 60; Joel R. Reidenberg, *Restoring Americans*, supra note 22, at 771.

THE CASE OF ON-LINE TERRITORIAL PRIVACY

To begin with, as a technological solution, 'gateway' or access-based zoning is used to restrict only private locales ex-ante, namely proprietary web sites. 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.¹²⁸ Without a gateway, interactions are effectively prohibited.¹²⁹ In fact, technology does not support an inherent distinction between public and private places, but instead only 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; as it decreases the level of accessibility and attractiveness of web sites that choose to independently fence themselves in. As a result, as some courts have already recognized, although gateway technology has been available on the World Wide Web for some time now, it is not available to all Web users,¹³⁰ and is just now becoming technologically feasible for chat rooms and USENET newsgroups.¹³¹ Gateway technology is not omnipresent in cyberspace, and because without it there is no means of age verification, most notably, cyberspace still remains largely unzoned--and unzoneable.¹³² As Court has recognized, for user-based zoning to be effectual, an agreed-upon code (or "tag") would have to be present; screening software or browsers with screening capabilities would have to be able to identify the "tag"; and those programs would have to be extensively available—and then widely used--by Internet users. At present, none of these circumstances prevail.¹³³ It is still the case that screening software "is not in wide use today" and "only a handful of browsers have screening capabilities."¹³⁴ There is, furthermore, no agreed-upon "tag" for those programs to identify.¹³⁵ 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.¹³⁶

Third, strict technologically based zoning is not backed by the Digital Millennium Copyright Act ("DMCA") protective measurements. Thus, it does not seem to invalidate the requirement for a contractual framework in case territorial privacy is ignored.¹³⁷ Originally, 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.¹³⁸ Under the DMCA, it is illegal to "circumvent a technological measure that effectively controls

¹²⁸ Reidenberg, *Governing Networks*, supra note 76, at 917.

¹²⁹ *Id.*, at 918;

¹³⁰ See, *Reno v. ACLU*, supra note 61, at 845; *Shea v. Reno*, 930 F.Supp. 916, 933-934 (S.D.N.Y.1996).

¹³¹ *Id.*, *Reno v. ACLU*, at 891.

¹³² See, *Id.*, p.846; *Shea v. Reno*, supra note 197, at 934.

¹³³ *Shea v. Reno*, *Id.*, at 945-946.

¹³⁴ *Id.*, at 945-946.

¹³⁵ See, *Reno v. ACLU*, supra note 61, at 848; *Shea*, supra note 197, at 945.

¹³⁶ See, *Reno v. ACLU*, supra note 61, at 845.

¹³⁷ For the alternative solution based on territorial privacy, see, also, discussion in Part III.C.2.a, *infra*.

¹³⁸ 17 U.S.C. §1201 (Supp. IV 1998).

THE CASE OF ON-LINE TERRITORIAL PRIVACY

access to a work protected" by copyright.¹³⁹ 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.¹⁴⁰ Most e-commerce web sites, 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.¹⁴¹ As a result, technological zoning assumes a contractual relationship, whereas due to the lack sufficient will and implementation of identification and contractual consent, such a solution is still inefficient. A territorially based solution instead would only necessitate unilateral notice at the entrance to on-line locales should be preferred, as it may overcome the need for identification and contractual consent.¹⁴² 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;¹⁴³ In public locales, however, observance should be freely allowed, as long as a notice of the public locale is brought forth, but then be solely restricted to the collection of non-identifiable registration and clickstream data.¹⁴⁴

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.¹⁴⁵ A localist boundary theory, thus, 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.¹⁴⁶ In the real world, this sort of dialogue between courts and lawmakers to delineate the geographic limits is the heart of what Farber calls in the context of international environmental law the evolutionary approach.¹⁴⁷ In the midst of a technological regulatory vacuum and due to the arguable sufficiency of the legal solution, this same approach, ultimately, should hold for cyberspace.

¹³⁹ *Id.*, at §1201(a)(1)(A).

¹⁴⁰ *Id.*, at §1201(a)(3)(B).

¹⁴¹ O'Rourke, Property Rights, *supra* note 43, at 583-584 and Fn 95 & accompanying text.

¹⁴² See, also, discussion in Part III.C.2.a, *infra*.

¹⁴³ Richard B. Parker, A Definition of Privacy, 27 Rutgers L. Rev. 275, 280 (1974); see also, Ruth Gavison, *supra* note 1, at 432-33.

¹⁴⁴ Richard B. Parker, *Id.*, at 280; See also, Ruth Gavison, *supra* note 1, *Id.*

¹⁴⁵ See, Christopher D. Stone, *supra* note 44, *Id.*

¹⁴⁶ *Thrift-Tel, Inc. v. Bezenek*, 54 Cal. Rptr. 2d 468, 473 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 personal property), at 473-74 (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 *Thrift-Tel* for support in finding electronic signals sufficient for trespass to chattels action).

¹⁴⁷ See, Daniel A. Farber, *supra* note 44, at 1273; Christopher D. Stone, *supra* note 44, *Id.*

c. *The sufficiency of legal solutions*

A functional subsistence of such a distinction between a public and a private sphere or locales of human activity, primarily, is a central tenet of jurisprudence in liberal democracy.¹⁴⁸ 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.¹⁴⁹ Notably, in the present service economy, information has become an increasingly valuable commodity.¹⁵⁰ That development eventually penetrated also the various legal fields and became impossible to ignore.¹⁵¹ Notably, as a legal concern, the private/public distinction also came to be

¹⁴⁸ For U.S. Federal courts upholding the difference between public sphere and private sphere, see, e.g., See, e.g., *United States v. Knotts*, 460 U.S. 276, 284 (1983) (discussing human activity in terms of public and private spheres) (citing *United States v. Knotts*, 662 F.2d 515, 518 (8th Cir. 1981)); *United States v. Bailey*, 628 F.2d 938, 941-43 (6th Cir. 1980) (noting distinction between activity in public and private spheres). See, also, Robert H. Mnookin, *supra* note 149, at 1429 (noting distinction between public and private spheres relating to individual rights vis-a-vis government powers).

¹⁴⁹ See, primarily, Trent Schroyer, *The Critique of Domination*. New York: George Braziller (1973); Jürgen Habermas, *Legitimation Crisis*, Trans. Thomas McCarthy. Boston: Beacon Press (1975); Andrew Fraser, *The Legal Theory We Need Now*, 1978 *Socialist Review* 147 (1978); Ellen Wood, Ellen Meiksins, *The Separation of the Economic and the Political in Capitalism*, 127 *New Left Review* 66 (1981).

¹⁵⁰ Patricia Mell, *supra* note 112, at 26-41 (While information has always been a core resource (referring to Anthony G. Oettinger, *Information Resources: Knowledge and Power in the 21st Century*, 209 *Science* 191, 191 (1980))

¹⁵¹ For different legal applications regarding the distinction, see, e.g., Karl Klare, E., *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); Isaac Balbus, *Commodity Form and Legal Form: An Essay on the Relative Autonomy of the Law*, 11 *Law & Society Review* 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, *supra* note 151 (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 retrospective, 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, also, Robert C. Ellickson, *supra* note 114, at 1381 et. al. Moreover, even Kennedy himself has reconsidered this approach. See Gabel & 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 is positive to suggest that such a distinction is no more 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", at 1349, 1350, *Id.* At least on this factual ground Kennedy's argument might seem to be too adventurous. See, e.g., Seidenman, arguing, in fact, that during the *Lochner* era an assumption of "natural" boundary was made in the Supreme Court. See, Louis Michael Seidman, *supra* note 159, at 1006; *Lochner v. New York*, 198 U.S. 45 (1905); For a supporting survey of the era, see G. Stone, L. Seidman, C. Sunstein & M. Tushnet, *supra* note 179, at 739-41.

THE CASE OF ON-LINE TERRITORIAL PRIVACY

known for its application on questions of legal jurisdiction, examining the mechanisms by which legal boundaries can be established and altered.¹⁵²

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, originally as in the constituting waterfront beach cases.¹⁵³ The first is a theory of 'custom,' where the public asserts ownership of property under some claim so ancient that it antedates any memory to the contrary.¹⁵⁴ Clearly, network environments such as the Internet are far too young to give rise to such ancient claims, such that antedates 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 future. Second is a prescriptive or dedicatory theory, by which a period of public usage gives rise to an implied grant or gift from private owners;¹⁵⁵ In cyberspace such a theory might turn to 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, and thus tortuously unobtrusive. The third is a 'public trust' theory, to the effect that the public always has rights of access to the property in question, and that any private rights are subordinate to the public's 'trust' rights;¹⁵⁶ Carol Rose calls such lands

Second, Kennedy is inherently not concerned with the exact substance of each sphere, but then assumes their practical existence. See, e.g., 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 vague or otherwise clear, any justification in ignoring the existence of boundary in between should only be possible in marginal extreme situations. See, also, discussion in Part III.B.1, hereafter.

¹⁵² See, e.g., Jeff Weintraub, *supra* note 159, at 9; Gerald E. Frug, *supra* note 172, *Id.*

¹⁵³ See, Curtis J. Berger, *supra* note 112, at 655-659.

¹⁵⁴ Carol Rose, *The comedy of the commons: Custom, commerce, and inherently public*, 53 U. Chi. L. Rev. 711, at 714 [Hereinafter, 'Rose, *The comedy of the commons*'] & Fn. 16, referring to Courts in Florida, Hawaii, and Oregon have adopted this approach. See *City of Daytona Beach*, 294 So. 2d 73 (Fla.); *County of Hawaii v. Sotomura*, 55 Hawaii 176, 517 P.2d 57 (1973), cert. denied, 419 U.S. 872 (1974); *In re Ashford*, 50 Hawaii 314, 440 P.2d 76 (1968); *Thornton*, 462 P.2d 671 (Or.).

¹⁵⁵ See, Rose, *The comedy of the commons*, *Id.*, at 714 & Fn. 15, referring to California's *Gion*, 465 P.2d 50. Other states in which courts have recently applied the 'implied dedication' or prescriptive approach to the waterfront are Texas, in *Seaway Co.*, 375 S.W.2d 923, and--somewhat reluctantly--New York, in *Gewirtz v. City of Long Beach*, 69 Misc. 2d 763, 330 N.Y.S.2d 495 (Sup. Ct. 1972), *aff'd*, 45 A.D.2d 841, 358 N.Y.S.2d 957 (1974) (mem.). Cf. *Department of Natural Resources v. Mayor of Ocean City*, 274 Md. 1, 332 A.2d 630 (1975) (doctrine held inapplicable because no clear intent to dedicate); *State v. Beach Co.*, 271 S.C. 425, 248 S.E.2d 115 (1978) (no intent to dedicate). For commentary, see, for example, 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); Comment, *Public or Private Ownership of Beaches: An Alternative to Implied Dedication*, 18 UCLA L. Rev. 795 (1971); Note, *This Land Is My Land: The Doctrine of Implied Dedication and Its Application to California Beaches*, 44 S. Cal. L. Rev. 1092 (1971).

¹⁵⁶ See, Rose, *The comedy of the commons*, *Id.*, at 714 & Fn. 14, referring to *State v. Superior Court*, 29 Cal. 3d 210, 625 P.2d 239, 172 Cal. Rptr. 696, cert. denied, 454 U.S. 865; *City of Berkeley*, 606 P.2d 362; *Van Ness*, 393 A.2d 571; *Borough of Neptune City*, 294 A.2d 47; *Matthews v. Bay Head Improvement Ass'n*, 95 N.J. 306, 471 A.2d 355, cert. denied, 105 S. Ct. 93 (1984); *Just v. Marinette County*, 56 Wis. 2d 7, 201 N.W.2d 761, 768-69 (1972).

For real world context, Note, *The Public Trust in Tidal Areas: A Sometime Submerged Traditional Doctrine*, 79 Yale L. J. 762 (1970); 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,

THE CASE OF ON-LINE TERRITORIAL PRIVACY

"inherently public property".¹⁵⁷ 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.'¹⁵⁸ Upholding the "Inherently public property" (jus publicum) doctrine, for this public to claim property, two elements were essential: first, the property had to be capable of monopolization by private persons, or would have been without doctrines securing public access against such threats.¹⁵⁹ Second, the public's claim had to be superior to that of the private owner, because the properties themselves were most valuable when used by indefinite and unlimited numbers of persons--by the public at large.¹⁶⁰ Courts have become receptive to requests to extend this technique 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 any number of types of property deemed public resources including parks,¹⁶¹ marshlands,¹⁶² archeological sites,¹⁶³ etc. In accordance with this result, Courts have distinctively adhered to public places as 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. As explained, the only way to balance that activity with private territorial privacy protection policies, as it is balanced in the real 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.¹⁶⁴

2. *Consciousness of Falsity*

Alternatively to a legal function, such as non-material locales, being a statement propounded with a recognition of utility – a legal fiction may incur complete or partial

see, also, Maureen Ryan, *supra* note 181, *Id*; Molly S. van Houweling, *Cultivating Open Information Platforms: A Land Trust Model*, 1 J. Telecomm. & High Tech. L. 309 (2002).

¹⁵⁷ Carol Rose, *The comedy of the commons*, *Id*, at 720.

¹⁵⁸ See, Rose, *The comedy of the commons*, at 715-716 and relevant footnotes for additional source, especially Fn. 10 & accompanying text.; referring to Scheiber, *Public Rights and the Rule of Law in American Legal History*, 72 Cal. L. Rev. 217 (1984); 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.

¹⁵⁹ *Id*, Rose, *The comedy of the commons*, at 774.

¹⁶⁰ *Id*, at 774.

¹⁶¹ See, e.g., *Paepcke v. Public Bldg. Comm'n*, 263 N.E.2d 11 (Ill. 1970); *Wade v. Kramer*, 459 N.E.2d 1025 (Ill. App. Ct. 1984); *Gould v. Greylock Reservation Comm'n*, 215 N.E.2d 114 (Mass. 1966).

¹⁶² See, e.g., *Freeborn v. Bryson*, 210 N.W.2d 290 (Minn. 1973).

¹⁶³ See, e.g., *San Diego County Archaeological Soc'y v. Compadres*, 81 Cal. App. 3d 923, 146 Cal. Rptr. 786 (1978) (holding that the public trust doctrine cannot be extended to cover archeological remains located on private property).

¹⁶⁴ David J. Goldstone, *supra* note 42, at 3.

THE CASE OF ON-LINE TERRITORIAL PRIVACY

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.¹⁶⁵ This should arguably, be also the experience of formalizing a localist boundary theory for cyberspace based on a legal fiction of locales. In continuation, there are two distinctions that narrow the subject matter of any legal fictions. The first is the distinction between a fiction and a lie.¹⁶⁶ A fiction is distinguished from a lie by the fact that it is not meant to deceive.¹⁶⁷ 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 herself believe the false statement. It is probably the case that, thus far, no such intentional lie was introduced into the boundary theory discourse regarding on-line spatiality. This distinction is, therefore less relevant to the present framework. The second and more relevant to cyberspace's spatiality discussion is the distinction between a fiction and an erroneous conclusion.¹⁶⁸ 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.¹⁶⁹ In such cases, the author of the legal fiction "either positively disbelieves it or is partially conscious of its untruth or inadequacy."¹⁷⁰ Along the lines of this distinction, scientific truism has given rise to many commentators in criticizing Courts for applying the doctrine of trespass to chattel, most notably, to cyberspace.¹⁷¹ Evidently, no statement, describing either the physical world or network environments can adequately describe reality. Fuller reserved the label of "false," however, only for those statements that are outstanding or unusual in their inadequacy.¹⁷² Once the label of "false" has attached, and the statement has been made with no intent to deceive, we have a legal fiction.¹⁷³ Accordingly, a statement must be false before it can be 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, rested upon the user's recognition of the statement's falsity, a distinction between 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

¹⁶⁵ See, e.g., *New England Divisions Case*, 261 U.S. 184, 197, 43 S.Ct. 270, 275, 67 L.Ed. 605 (1923); *Railroad Comm'n of Wisconsin v. Chicago, Burlington & Quincy R. Co.*, 257 U.S. 563, 579, 42 S.Ct. 232, 234, 66 L.Ed. 371 (1922). See, also, Chief Judge, United States Court of Appeals for the Federal Circuit, Howard T. Markey, *Jurisprudence or "Jurisience"?*, *William and Mary Law Review* 525 (1984), at 525-526.

¹⁶⁶ L. Fuller, *supra* note 131, at 7. See, also, *Federal Power Commission v. Florida Power & Light Co.*, 92 S.Ct. 637 U.S. Fla. 1972. Decided Jan. 12, 1972; 405 U.S. 948, 92 S.Ct. 929 (Reversed and remanded) (rejecting a jurisprudential approach that meets the standard at law, but it is technologically unsound), p. 459. See, also, discussion at Part II.C.1.b, *infra*.

¹⁶⁷ *Id.*

¹⁶⁸ *Id.*

¹⁶⁹ *Id.*

¹⁷⁰ L. Fuller, *supra* note 131, at 8.

¹⁷¹ Hunter, *supra* note 43; Maureen A. O'Rourke, *supra* note 43, at 595-97; Dan Burk, *The Trouble With Trespass*, at 34 [Hereinafter, 'Burk, *The Trouble With Trespass*'].

¹⁷² L. Fuller, *supra* note 131, at 11-12.

¹⁷³ *Id.*

THE CASE OF ON-LINE TERRITORIAL PRIVACY

consciousness of its falsity".¹⁷⁴ Fuller considered such a legal fiction benign.¹⁷⁵ 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 technically locales do not subsist on-line, or to say that their existence, instead, is legally fictional. The latter approach could be then justified either because technology is not capable or partly technically immature enough to uphold on-line spatiality or self-regulated differentiated locales, in their strict scientific sense, as is presently the case in cyberspace.¹⁷⁶

Even if a legal fiction of on-line locales is finally agreed upon, technically it might still 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 in controlling disclosure of use of personal information directly conflicts with the concept of public distribution of information.¹⁷⁷ Yet, as important as it 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 imminent for a liberal democratic society to agree on the existence of such a distinction in the first place.¹⁷⁸ Thus, even the ambiguity regarding the appropriate *location* of a boundary between locales is not a unique concern to the digital era.¹⁷⁹ Occasionally, even before the information age, it has been a source of controversy.¹⁸⁰ Since the realist movement in American jurisprudence in the 1930's,¹⁸¹ the boundary's ambiguity has become increasingly obvious.¹⁸² In dealing with this issue, it should be clear at the outset that the system will never operate as cleanly as do the rules governing property rights on land.¹⁸³ As Richard Epstein points out, for land disputes it is generally clear when one person has crossed the boundary that separates his or her property from another.¹⁸⁴ The definition and identification of appropriate boundaries is never as clear in disputes over privacy.¹⁸⁵

¹⁷⁴ *Id.*, at 10.

¹⁷⁵ *Id.*

¹⁷⁶ On the institutional explanation for this argument, see discussion in Part III.C.2, *infra*.

¹⁷⁷ See, e.g., Raymond T. Nimmer, *supra* note 1, ¶ 8.05.

¹⁷⁸ See, e.g., Solove, *Conceptualizing Privacy*, *supra* note 9, at 1132.

¹⁷⁹ See, e.g., Patricia Mell, *supra* note 112, at. 4, 22.

¹⁸⁰ See, Mnookin, *The Public/Private Dichotomy: Political Disagreement and Academic Repudiation*, 130 U. Pa. L. Rev. 1429, 1429 (1982), at 1430-34 (discussing various definitions of dividing line between public and private spheres).

¹⁸¹ For a general description of the realist challenge to formalism that began in the 1920's, see Mensch, *The History of Mainstream Legal Thought*, in *The politics of law: A progressive critique* 26-29 (D. Kairys ed. 1982).

¹⁸² 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 Held at the University of Pennsylvania on January 20, 1982*, 130 U. PA. L. Rev. 1289-1602 (1982); Duncan Kennedy, *The Stages of Decline of the Public/Private Distinction*, 130 U. PA. L. REV. 1349, 1349 (1982).

¹⁸³ See, Richard A. Epstein, *Deconstructing Privacy: And Putting it Back Together Again*, In *The Right to Privacy*, Elen Frankel Paul, Fred D. Miller, Jr., and Jeffrey Paul eds., (Cambridge University Press, 2000) 1, at 7

¹⁸⁴ *Id.*

¹⁸⁵ *Id.*

THE CASE OF ON-LINE TERRITORIAL PRIVACY

This legal intricacy only continued the tension that existed in earlier telecommunications systems.¹⁸⁶ Especially notable is the merging of telephone and television with computers that has resulted in the development of a flexible and diverse international information-exchange system which allowed the nearly instantaneous transfer of information through cables, satellites, microwave relays and fiber optics.¹⁸⁷ Nevertheless, simply by maintaining a positivistic right to privacy, both initially uphold the constituting framework of jurisdictional boundaries and thus the need for an inner balance between private and public rationales.¹⁸⁸ Thus, even accepting these certainty limitations, it is possible to make some measurable progress to a sensible end.¹⁸⁹ 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.¹⁹⁰ The legal fiction of on-line locales, can, thus, still be seen *benign* assuming that it is to be 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, indeed, very popular in American jurisprudence and should therefore not be considered extraneous or passé by cyber lawyers.¹⁹¹ Presumptions, and the associated burdens of proof necessary to overcome them, presently appear virtually everywhere in law.¹⁹² In property law, for example, a specific legal fiction is the presumption that one who owned soil owned all the way to the heavens and to the depths.¹⁹³ In employment discrimination

¹⁸⁶ See, e.g., Daniel Bell, Communications Technology--For Better or for Worse, *Harv. Bus. Rev.*, May-June 1979, at 20, at 21.

¹⁸⁷ *Id.*

¹⁸⁸ For the view suggesting that the private/public distinction involves especially questions of jurisdiction, 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* (Jeff Weintraub and Krishan Kumar, eds) (University of Chicago press, 1997) 1, at 9.

¹⁸⁹ See, Richard A. Epstein, *supra* note 151, at 7.

¹⁹⁰ Louis Michael Seidman, *Public Principle and Private Choice: The Uneasy Case for a Boundary Maintenance Theory of Constitutional Law*, *Yale L.J.* 1006 (1987), at 1007.

¹⁹¹ For the leading scholarship on Legal Fictions are, G. Calabresi, *Ideals, beliefs, attitudes, and the law: Private law perspectives on a public law problem* (1985); G. Calabresi, *A common law for the age of statutes* 172-77 (1982); Abrams, *A Constitutional Law for the Age of Anxiety* (Book Review), 73 *Calif. L. Rev.* 1643 (1985); Block, *Suits Against Government Officials and the Sovereign Immunity Doctrine*, 59 *Harv. L. Rev.* 1060 (1946); Note, *Penumbras and Privacy: A Study of the Use of Fictions in Constitutional Decision-Making*, 89 *W. VA. L. Rev.* 859 (1985); Ronald J. Allen, *Burdens of Proof, Uncertainty, and Ambiguity in Modern Legal Discourse*, 17 *Harvard Journal of Law and Public Policy* 627 (1994). For some reason, however, interest cooled down until the 1920's when Roscoe Pound, John Chipman Gray, and Lon Fuller reawakened this dormant jurisprudential technique. Louise Harmon, *Falling Off the Vine: Legal Fictions and the Doctrine of Substituted Judgment*, *Yale L. J.* (1990) 1, at 11.

¹⁹² See R. Pound, *Interpretations of legal history* 131 (1923); L. Fuller, *supra* note 131, at 1; Wilkinson, J. Harvie III., *Toward a Jurisprudence of Presumptions*, 67 *N.Y.U. L. Rev.* 907 (1992), at 907; Aviam Soifer, *Reviewing Legal Fictions*, 20 *Ga. L. Rev.* 871 (Summer, 1986), at 872, 875; Antonio E. Bernardo & Ivo Welch, *A Theory of Legal Presumption*, 16 *J. L. ECON. ORG.* (April 2000) 1, at 2.

¹⁹³ C. Donahue, JR., T. Kauper, & P. Martin, *Cases and materials on property* 291 (1974). See generally W. Empson, *Seven types of ambiguity* (1930), and the extensive work by Owen Barfield, including in

THE CASE OF ON-LINE TERRITORIAL PRIVACY

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 was a qualified (but rejected) applicant and a member of a historically oppressed group.¹⁹⁴ 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.¹⁹⁵ A legal fiction is commonly seen as an assumption which conceals, or affects to conceal, the fact that a rule of law, such as differentiated private and public on-line locales, has undergone alteration, such as in cyberspace, yet its letter remained unchanged.¹⁹⁶ Thus the fiction of "inviting" in the "attractive nuisance" cases is intended to escape the rule that there is no duty of care toward entrants.¹⁹⁷ 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.¹⁹⁸ There are truly few absolute principles in law.¹⁹⁹ Those principles that may appear to be absolute are, in reality, presumptions, which may be overcome in appropriate circumstances.²⁰⁰ Arguably, the time has come for theoreticians and policy makers alike to reevaluate the present anti-globalists and globalist paradigms of cyberspace and ultimately integrate territorial privacy to 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 physical world's notion of geographic spatiality, it being 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.²⁰¹ First, it must be based on an inference justified by common experience, based on absence of other proof and as drawn from available evidence.²⁰² Second, it must be phrased in realistic terms; order, not an

particular, Poetic Diction and Legal Fiction, in O. Barfield, *The rediscovery of meaning, and other essays* 44 (1977).

¹⁹⁴ See, *McDonnell-Douglas v. Green*, 411 U.S. 792 (1973).

¹⁹⁵ See, Gunther, Gerald, and Kathleen Sullivan, *Constitutional Law* (1998). Lon Fuller reminds us of many more examples, such as constructive delivery in contract law. See, L. Fuller, *supra* note 131, at 15; and implied provisions in contracts. L. Fuller, *Id.*, at 8.

¹⁹⁶ Maine, *Ancient Law*, in *The problem of jurisprudence* 371 (L. Fuller ed. 1946) (chapter reprints first half of H. 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 161, at 131; L. Fuller, *Supra* note 131, at 53.

¹⁹⁷ L. Fuller, *id.*, at 53.

¹⁹⁸ Wilkinson, J. Harvie, *supra* note 161, at 907.

¹⁹⁹ *Id.*

²⁰⁰ *Id.*, at 907, 908.

²⁰¹ L. Fuller, *supra* note 131, at 45 et al.

²⁰² *Id.*

THE CASE OF ON-LINE TERRITORIAL PRIVACY

“inference”, but a disposition of the case in a certain contingency.²⁰³ Lastly, be freely rebuttable.²⁰⁴ This part will analyze these three conditions, while overcoming the constituting globalist and anti-globalist boundary claims in opposition to the possibility of legally acknowledging on-line locales in cyberspace.

1. *Based on an inference justified by common experience*
 - a) *Absence of other proof*

The first among the two conditions a fiction or a presumption must be based on as an inference justified by common experience is that it has to be based on an absence of other proof.²⁰⁵ 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.²⁰⁶ Sometimes the reason for tolerating a gap either between evidence and findings or between findings and decision has to do with limitations of human intellects or limitations on the magnitude of investigations that may be conducted in particular circumstances. In application of this standard, courts have already acknowledged that based on 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. That is, even in an analogous concern to cyberspace's spatial discourse, such as when upholding interstate commerce based on the evidential question of how electricity actually moves in a bus.²⁰⁷ In balance, though, not all propositions of fact that is useful and used in the administrative process are susceptible of proof with evidence.²⁰⁸

Overcoming the constituting globalist and anti-globalist boundary claims against the possibility of legally acknowledging on-line locales, is made here in two levels. A form of heterogeneity involving the requirement of a physical presence threatens the first weakness of the homogenous definition of space in its globalist boundary theory sense. Arguably, localist boundary theory may overcome the physical world's wrong analogy upheld as scientific truism, which suggests that locales and the physical nexus of individuals to them must be physical.²⁰⁹ The second weakness of the homogenous globalist boundary sense that may overcome by a form of heterogeneity involves the

²⁰³ *Id.*

²⁰⁴ *Id.*

²⁰⁵ *Id.*

²⁰⁶ See, e.g., *Federal Power Commission v. Florida Power & Light Co.*, supra note 135, at 465-466.

²⁰⁷ *Id.*

²⁰⁸ See, e.g., *FPC v. Southern California Edison Co.*, 376 U.S. 205, 209 n. 5, 84 S.Ct. 644, 647, 11 L.Ed.2d 638 (1964); *Travelers' Indemnity Co. v. Parkersburg Iron & Steel Co.*, 70 F.2d 63, 64 (1934); *United States ex rel. Chapman v. FPC*, 191 F.2d 796, 808 (1951) aff'd, 345 U.S. 153, 73 S.Ct. 609, 97 L.Ed. 918 (1953). See, also, 7 J. Wigmore, *Evidence* §§ 1917--1929, 1976 (3d ed. 1940 and Supp. 1970).

²⁰⁹ Thus, as explained in outset of part II, operationally, the extent of a territory can be defined by the set of points within it. P. Haggett, supra note 126, at 40-55. In non-physical environments, political geography therefore allows us to uphold a one-point locale that, in essence, becomes non-physical. The emphasis on physical presence naturally originates in the real world's application of localist boundary theory. See, Daniel A. Farber, supra note 44, at 1270; Soja, *A paradigm*, at 53. See, also, discussion, herein.

THE CASE OF ON-LINE TERRITORIAL PRIVACY

concern over discontinuities in the ability to interact between other spaces, namely the real world and among inner locations.²¹⁰ Localist boundary theory applied through a legal fiction of an on-line locale may arguably entail the existence of relations between locales – yet, without intrinsically involving geographical continuation, as will be explained herein.²¹¹

- 1) *First heterogeneity: Physical presence*
- i. *Non-physical locality*

Localist boundary theory is confronted with the wrong notion of the physical world that locales and the physical nexus of individuals to them must be physical. For a start, in regard to locales, we are told, 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.²¹² In analogy, to previous telecommunications networks, we are told, most Internet users access the Internet through a dial-up modem, converting digital data to analog sounds that can be sent over a telephone line just like the human voice.²¹³ There were computer networks before the Internet that similarly relied on telephonic exchange of data.²¹⁴ 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 don't exist as spaces, but instead as communications mediums.²¹⁵ Support for the physicality of locales, in fact, originates in public international law; which upholds that even the smallest 'area of land' must be 'natural' land as such that is capable of legal appropriation.²¹⁶ To be capable of appropriation an island territory, in fact, must present at high tide a surface of land clear of the water, which is large enough to be habitable in

²¹⁰ See, e.g., Hastings Donnan & Thomas M. Wilson, *supra* note 51, at 9.

²¹¹ *Id.*

²¹² Andrew L. Shapiro, *The Control Revolution: How the Internet Is Putting Individuals in Charge and Changing the World We Know* (1999), at 710-712 (cyberspace is not a real place but just a medium that we may control) [hereinafter, 'Shapiro, The Control Revolution']; Shapiro, *The Disappearance of* at 709 and see Fn. 21 & accompanying text; Timothy Wu, *When Law & the Internet First Met*, 3 *Green Bag 2d* 171 (1999-2000).

²¹³ For a discussion of the prevalence of private "bulletin board systems" in the late 1980s and early 1990s, see, e.g., 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).

²¹⁴ *Id.*

²¹⁵ Shapiro, *The Control Revolution*, *supra* note 243 (for the legal perspective), at 710-712; Timothy Wu, *supra* note 243 (same). See, also, Edward W. Soja, *Postmodern Geographies: The Reassertion of Space in Critical Social Theory* (1989) (For the political geography perspective).

²¹⁶ Article 121 of the Montego Bay Convention of 10 December 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'. See Monique Chemillier-Gendreau, *Sovereignty over the Paracel and Spratly islands* (Kluwer law international, 1996), at 22, referring to Laurent Lucchini & Michel Voelckel, *Droit de la mer*, vol. I (Paris, Pedone, 1990), at 331.

THE CASE OF ON-LINE TERRITORIAL PRIVACY

practice.²¹⁷ In resemblance to cyberspace scientific truism, this pragmatic notion of placeless seems to have led some public international law scholars in the real world all the way to insist that the islands must also be shown on geographical maps.²¹⁸ Adopting a not less pragmatic approach, however, the Anglo-American legal system, has consistently acknowledged alternative non-physical forms of discontinuous localized spatiality, and in various constitutional contexts. In seminal First Amendment cases such as *Perry*²¹⁹ and *Cornelius*,²²⁰ in the course of declaring them non-public forums, court went on identifying the relevant locales as a school district's internal mail system and a charity fund drive among federal employees, respectively, notwithstanding that each "lacks a physical situs."²²¹ In another context, in *United States v. Grace*,²²² the Court divided the Supreme Court grounds into perimeter sidewalks and interior grounds,²²³ relying on the sidewalks' functional continuity with the adjoining streets²²⁴ and indistinguishability from other public walkways.²²⁵ 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 instead made functional. Any remaining doubts that such a functionally defined locale could qualify as a public forum were dispelled in *Rosenberger*,²²⁶ where the Court characterized the university's student activity funding system as "open[ing] a limited forum"²²⁷ 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".²²⁸ With this jurisprudential shift in emphasis from what was, up till then, 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.²²⁹

²¹⁷ International Court of Justice, 1953, at 49, 53.

²¹⁸ See Monique Chemillier-Gendreau, *supra* note 247, at 22, referring to Gilbert Gidel, *La mer territoriale at la zone contigue*, (1934) *Recueil des Cours de l'Academie de Droit International*, II, vol. 48, at 137-278.

²¹⁹ *Perry Educ. Ass'n. v. Perry Local Educators' Ass'n.*, 460 U.S. 37 (1983).

²²⁰ *Cornelius v. NAACP Legal Defense and Educ. Fund, Inc.*, 473 U.S. 788 (1985).

²²¹ *Id.*, at 801.

²²² 461 U.S. 171 (1983).

²²³ *Id.*, at 179-80.

²²⁴ *Id.*, at 180.

²²⁵ *Id.*, at 179.

²²⁶ *Rosenberger v. University of Virginia*, 515 U.S. 819 (1995).

²²⁷ *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." *Id.*; *ISKCON*, 505 U.S. 672, 678 (1992). See *infra* Part II.A.2.

²²⁸ *Rosenberger v. University of Virginia*, at 830.

²²⁹ *Rosenberger v. Rector and Visitors of Univ. of Va.*, 515 U.S. 819, 830, 115 S.Ct. 2510, 2517, 132 L.Ed.2d 700 (1995) (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).

THE CASE OF ON-LINE TERRITORIAL PRIVACY

The notion of ‘territorial trap’ as posited by John Agnew has been an important statement 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’.²³⁰ The legal concern revolving accessibility to locales would therefore 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 functionally based analysis entails (and only then), there must be no inherent objection to why should our legal system not fictitiously expand the notion of locales into other virtual realms, such as cyberspace.

ii. *Imperfect geographic nexus*

The physical presence prerequisite has also been overcome in regard to the geographic nexus requirement. In the real world, that predominantly has been the case in standing to sue in environmental and land use cases in the federal courts.²³¹ Initially, in *Lujan v. National Wildlife Federation*, for example, the Supreme Court required a “geographic nexus” between the injured plaintiff and the specific area endangered by agency action, even though the Court couched its argument regarding the nexus’s degree of specificity in terms of “actually affected, without exhausting the forms of causality to physical ones.”²³² In continuation, 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 with (“vocational nexus”) or interest in an endangered animal (“animal nexus”) or habitat (“ecosystem nexus”) and an agency’s pending action.²³³

Further non-physical expansion of the nexus’ specificity followed in *Idaho Conservation League v. Mumma*.²³⁴ Distinguishing the National Wildlife Federation’s specificity requirement, the Ninth Circuit held that the plaintiffs satisfied the “geographic nexus”

²³⁰ Newman, *From Moribund Backwater*, supra note 97, at 16, referring to J. Agnew & S. Corbridge, *Mastering space: Hegemony, territory and international political economy* (London: Routledge, 1995), p. 79. Peter Tylor, as it relates to the state and the organization of non-physical power, also discusses the alternative understandings of territory, in his rejection of traditional physical notion of ‘territorial absolutism’. See, David Newman, at 16, *Id.*, referring to P.J. Tylor, *Territorial absolutism and its evasions*, *Geography research forum*, 16.

²³¹ 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, also Laurence H. Tribe, *American Constitutional Law*, §§ 3-15 to -17 (3rd ed. 2000), and primarily § 3-17, at 392-424.

²³² 497 U.S. 871, 885-89 (1990). See, also, *Sabine River Authority v. U.S. Dept. of Interior*, 951 F.2d at 675 (quoting *Lujan v. National Wildlife Fed’n*, (emphasis in original)).

²³³ 112 S. Ct. 2130, 2139-40 (1992).

²³⁴ 956 F.2d 1508, 1517 (9th Cir. 1992); see *National Wildlife Fed’n*, 497 U.S. at 882.

requirement despite their inability to specify threatened areas because the proposed development areas had not yet been determined.²³⁵ In their dissent in *Defenders*, Justices Blackmun and O'Connor further espoused and advanced the ecosystem nexus theory, acknowledging "(m)any environmental injuries...cause harm distant from the area immediately affected by the challenged action... such as rivers running long geographical courses."²³⁶ Likewise, the dissent impliedly endorsed the "animal nexus" theory in stating, "Environmental destruction may affect animals traveling over vast geographical ranges."²³⁷ The imperfect nexus between geographically compact districts or locales and communities of interest was finally acknowledged in *Prosser v. Elections Board*,²³⁸ in which the district court adopted its own apportionment plan for Wisconsin. Judge Posner held there that there is not a complete correlation between geographical propinquity and community of interests.²³⁹ In support of this imperfect nexus-requirement the courts, instead, warns us against the possible results of rigid scientific truism, suggesting that the achievement of perfect contiguity and compactness would only imply ruthless disregard for other elements of homogeneity; and would require breaking up counties, towns, villages, wards, even neighborhoods.²⁴⁰ To conclude, with this jurisprudential shift in emphasis from what was, up till then, perceived as a classic physical analysis towards a more functional one – locales and the physical nexus of individuals to them are indeed apparent 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 heterogeneity involving discontinuities in the ability to interact between other spaces, namely the real world and among inner locations.²⁴¹ From a legal perspective it entails the existence of relations between locales, yet without intrinsically involving geographical continuation.²⁴² This lack of continuous homogeneity, ultimately, upholds the legal notions of territory and borders.²⁴³ Firstly,

²³⁵ *Idaho Conservation League v. Mumma* 956 F.2d 1508, 1517 (9th Cir. 1992) (upholding a geographic nexus requirement in the Forest Service's). See, also, *City of Los Angeles v. National 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).

²³⁶ *Defenders*, 112 S. Ct. at 2154.

²³⁷ *Id.* (citing, for example, *Japan Whaling Ass'n v. American Cetacean Soc'y*, 478 U.S. 221 (1986)).

²³⁸ 793 F. Supp. 859 (W.D. Wis. 1992). *Id.* at 861-62.

²³⁹ 28 U.S.C. § 2284 (1994).

²⁴⁰ *Prosser*, supra note 268, at 863. See, also, *Public Citizen v. U.S. Trade Representative*, 822 F. Supp. 21, 28 (D.D.C. 1993) (citing *United States v. SCRAP*, 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 (§ 101, 16 U.S.C. § 1371 (1994)) are too widespread to be confined to a particular geographical location." In support, the district court 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'"), *Id.*

²⁴¹ See, e.g., supra note 51, at 9.

²⁴² *Id.*

²⁴³ See, e.g., *Hastings Donnan & Thomas M. Wilson*, supra note 51, at 9.

THE CASE OF ON-LINE TERRITORIAL PRIVACY

through the definition of territory - the political definition of a space that constitutes the core of geopolitical analysis.²⁴⁴ It also wove together areal 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. A system of settlements or central locales, for example, would consist of locations tied together by certain shared or complementary attributes (e.g., size, proximate location, types of services performed, socio-cultural features) and the structuring of interactions between them (e.g., flow of money, influence, people, goods and information).²⁴⁵ Secondly, 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, be they states, urban neighborhoods or group turfs, within which human activity takes place and is differentiated.²⁴⁶ By drawing boundaries around space considered theirs, people (and nations) strive to transform space into locales.²⁴⁷ Such boundaries are described in words or a treaty, shown on a map, or marked on the ground by physical indicators.²⁴⁸

In opposition to acknowledging both inner and outer borders in cyberspace, scientific truism largely upholds today that “in the strict technological sense”²⁴⁹ there is no empirical support for the spatiality paradigm,²⁵⁰ and courts, thus far, provided none.²⁵¹ Instead, a number of courts have made the mistake of overlooking the differences between the Internet and real space in a variety of contexts, such as when the doctrine of trespass to chattels to email and Web site access was applied, while assuming *inner*

²⁴⁴ 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. P. Haggett, *Locational analysis of human geography* (London: Arnold, 1965), 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 subjected to some level of control. They should, therefore, be more closely related to the analysis of territories than that of fields. See, also, discussion at Part III.C.2, *infra*.

²⁴⁵ Soja, A paradigm *supra* note 45, at 53.

²⁴⁶ Prescott, *Political geography* (Methuen & Co. Ltd, 1972), at 54, 61-74 [Hereinafter, ‘Prescott, Political geography’]; Suzanne Lalonde, *supra* note 124, at 8 and mentioned sources; J.R.V. Prescott, *Political frontiers and boundaries* (London: Unwin Hyman, 1987), at 36 [Hereinafter, ‘Prescot, Political frontiers’]; L.K.D Kristof, *supra* note 124, at 127; T. Cresswell, *In place, out of place: Geography, ideology and transgression* (University of Minnesota Press, 1996), at 149. In the physical world, with no appropriate analogy to network environments, Borderland is then ‘the transition zone within which the boundary lies’. See Prescott, *Political frontiers* *supra* note 124, at 13-14.

²⁴⁷ Stanley Waterman, *States of Segregation, 57-75*, In Clive Schofield, David Newman, Alasdair Drysdale & Janet Brown (eds.), *The Razor’s Edge: International Boundaries and Political Geography* (Kluwer Law International, 2002), at 63.

²⁴⁸ *Id.*

²⁴⁹ Dan Hunter, *supra* note 43, at 472; Mark Lemley, *supra* note 43, *id.*

²⁵⁰ See, O’Rourke, *Property Rights*, at 592 and Fn. 62, referring to Robert G. Sachs, *supra* note 90, at 1; Alfred C. Yen, *western Frontier of Feudal Society?: Metaphors and Perceptions of Cyberspace*, 17 *Berkeley Tech. L.J.* 1207 (2002), at 1216.

²⁵¹ See, Dan Hunter, *supra* note 43, at 472; Mark Lemley, *supra* note 43.

THE CASE OF ON-LINE TERRITORIAL PRIVACY

bordering.²⁵² 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.²⁵³ Neither, are we often told, is there empirical support for the notion of Cyberspace's "separateness" through *outer* bordering from physical space.²⁵⁴ These observations are, nevertheless, minor from the individual's perspective that entails human behavior which law regulates, regardless of the choice of legal fictions, on two levels. First, already 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 the history of claims of intrinsic sovereignty of national groups over island territories, the argument based on geographical 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.²⁵⁵ In the physical world, these observations are also minor concerning the type and use of the neighboring locale. In fact, discontinuation between locales due to 'spot zoning' or a zoning ordinance, which creates 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.²⁵⁶ It is of social and private interest to the parties involved in its use, and whenever there is a reasonable basis to treat the spot-zoned property differently from the surrounding property, spot zoning is valid.²⁵⁷ 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 be overcome by localist boundary theory also based on analogous experience among network environments that predated cyberspace. In international monetary wiring networks, the format and order in which information is

²⁵² For courts applying the doctrine of trespass to chattels to the Internet, see, e.g., *America Online v. National Health Care Discount, Inc.*, 174 F. Supp. 2d 890 (N.D. Iowa 2001); *Oyster Software, Inc. v. Forms Processing*, 2001 WL 1736382 (N.D. Cal. 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 (Cal. Ct. App. 2001), review granted, 43 P.3d 587 (Cal. 2002). For early use of the trespass doctrine to computers, see, e.g., *People v. Versaggi*, 83 N.Y.2d 123, 129 (1994) (noting the New York state legislation proscribing computer trespass, Penal Law § 156.10). 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).

²⁵³ See, e.g., Hunter, *supra* note 43 (criticizing the courts' application of the cyberspace as place metaphor); O'Rourke, *Analogy*, *supra* note (criticizing courts for creating a broad property right on information for network environments), pp. 595-97; Burk, *The Trouble With Trespass* (criticizing courts ignoring the damage requirement of trespass to chattels to network environments), p. 34.

²⁵⁴ See, O'Rourke, *Property Rights*, *supra* note 43, at 592 and Fn. 62, referring to Robert G. Sachs, *supra* note 90, at 1.

²⁵⁵ See Monique Chemillier-Gendreau, *supra* note 247, at 27-29 and Fn. 20-23 & accompanying text.

²⁵⁶ *Little v. Winborn*, Supreme Court of Iowa (1994) 518 N.W. 2d 384, referring to *Jaffe v. City of Davenport*, 179 N.W. 2d 554, 556 (Iowa 1970). See, also, 8 E. McQuillen, *Municipal Corporations* § 25.84, at 319 (3rd ed. Rev. 1991).

²⁵⁷ *Little v. Winborn*, Supreme Court of Iowa, 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, *Id*

THE CASE OF ON-LINE TERRITORIAL PRIVACY

stored does not diminish its tangibility and logical retrieval, whenever it is assembled and presented to the user as cohesive essence. There as well, the appropriate nature of data storage is 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 signifies a sum of money at a bank account, or a check legal obligation that is 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" that meetings in Cyberspace may become a viable alternative to meetings in physical space.²⁵⁸ That is, regardless of the format and order in which information is stored. In a 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.

There are however, a few indications that a shift toward 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"²⁵⁹ Instead of relaxing the discontinuous localist spatial analogy with the prevailing technocentric 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 real 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. That is, 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,²⁶⁰ but also to how the nature of the Internet might change over time in ways that affected its regulability.²⁶¹ Almost anecdotally, recognition of the homogenous weakness concerning continuity, ultimately, can be found within Johnson and Post's globalist argument. In fact, less attention has thus far given to the fact that Johnson & Post's boundary approach, normatively accepts the possibility of *inner* bordering within distinct Cyberspace locales (or "constellations"²⁶² or "areas"²⁶³).²⁶⁴ Each

²⁵⁸ See, I. Trotter Hardy, *Electronic Conferences: The Report of an Experiment*, 6 Harv. J.L. & Tech. 213, 232-34 (1993) (discussing the advantages of e-mail conferences) (Fn. 30) [Hereinafter, 'Hardy, *Electronic Conferences*'].

²⁵⁹ See, *Reno v. ACLU*, supra note 61, at 2354.

²⁶⁰ *Id.*, at 889-90 (O'Connor, J., concurring).

²⁶¹ *Id.*, at 890 (O'Connor, J., concurring). See also Lawrence Lessig, supra note 68, at 886-89; Lawrence Lessig & Paul Resnick, supra note 72; O'Connor's concurrence has been criticized as a rote application of the cyberspace as place metaphor, however. See Josh A. Goldfoot, supra note 88, at 920-21.

²⁶² Johnson & Post, supra note 59, at 1379 and Fn. M92-96 and accompanying text.

²⁶³ *Id.*

²⁶⁴ In a conversation with David Post he further suggested that the 'inner zoning' argument should have been understood as even more acute that the more cited 'outer zoning separateness' argument vis-à-vis the real world. (Interview with David Post 3/12/04). Post's localist heterogeneous clarification, however, remains in tension with his main argument that views cyberspace as a global spatial system, regardless of its relation to the real world spatiality.

THE CASE OF ON-LINE TERRITORIAL PRIVACY

such virtual locale, as they normatively agree, could then likely develop its own set of distinct rules.²⁶⁵ Thus, as localist boundary theory predicts, conduct acceptable in one locale of cyberspace could then be fenced-out by another.²⁶⁶ Albeit, once again, based on a technocentric approach, in due course, so does Johnson & Post's approach could succumb to the prospect of localist discontinuity as much as technology allows.²⁶⁷ 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*

A second weakness of the homogenous definition of space according to globalist boundary theoreticians is threatened by heterogeneity due to the existence of distance²⁶⁸ and its influence on entry preferences on individuals.²⁶⁹ 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.²⁷⁰ Scientific truism rejects the soundness of these localist boundary theory propositions for cyberspace on several levels. Firstly, we are told, whereas a physical locale assumes ability to enter it, network environments are said not to have that ability, as entering a web site is physically impossible. Instead, we are told, only a replacement of data exists.²⁷¹ As Lemley all-purposely suggests, courts have not understood that no one "enters" Web sites.²⁷² Instead, relevant on-line trespass cases' defendants merely send request for information to a web server, which the plaintiff had made open to the public, and the plaintiff's own server sends information in return.²⁷³ 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 and as such entails further spatial disparity from the physical world's spatial analysis. To begin with, multiple entries/entrants is said to diminish the stability of

²⁶⁵ Johnson & Post, *supra* note 59, at 1379.

²⁶⁶ *Id.*, at 1379, 1396-1397.

²⁶⁷ In further continuation 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. See, *Id.*, at 1379 and Fn. 33 & accompanying text.

²⁶⁸ Legal appliance 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. J.R.V. Prescott, *Political geography*, *supra* note 105, at 54, 56-61; Suzanne Lalonde, *Determining boundaries in a conflicted world* (McGill-Queen's University Press, 2002), at 8 and mentioned sources; L.K.D Kristof, *The nature of frontiers and boundaries*, In R.E. Kasperson & J.V. Minghi (eds.), *The structure of political geography* (Chicago: Aldine, 1969), p. 127. Frontiers are of less importance to network environments, as will be explained herein.

²⁶⁹ J.R.V. Prescott, *supra* note 105, at 54, 56-61; Suzanne Lalonde, *supra* note 124, at 8 and mentioned sources; L.K.D Kristof, *supra* note 124, at 127.

²⁷⁰ *Id.*

²⁷¹ Mark Lemley, *supra* note 43, *Id.*; Shapiro, *The Disappearance*, at 710.

²⁷² *Id.*

²⁷³ Mark Lemley, *Id.*

THE CASE OF ON-LINE TERRITORIAL PRIVACY

locations.²⁷⁴ In addition, it is said to override passage scarcity, as for on-line communications purposes bandwidth is effectively infinite.²⁷⁵ Secondly, in network environment observance is said to be impossible, as it lacks the concept of proportional proximity or “next door”.²⁷⁶ Thus, as scientific truism argues, there can be no non-material public locales, such as streets or sidewalks, from which to observe on either public or private spheres could be made possible.²⁷⁷

Analyzing localist boundary theory as legal truth may, however, 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."²⁷⁸ 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 not even indispensable. In the following regard it is the case that 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 matters presented to them.²⁷⁹ Based on a conventional framework of legal fiction of 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. That is, for reasons deriving from an analogy to the real world’s remote access and the added *reverse* remote access nature of cyberspace.

To begin with, in comparing non-physical electronic access to physical access there is still a sufficient level of scientific truth analogy that could permit us to overcome the obstacle set by this argument, in two levels. Firstly, the existence of non-physical entry should not be seen unique to network environments, and should be legally analogized to physical environments. In the latter, the requirement of actual trespass was largely abandoned with the tort of privacy intrusion.²⁸⁰ Thus, 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,²⁸¹ and in different circumstances parents were liable to long-distance telephone company for trespass to personal property arising from their sons' unauthorized use of confidential codes to gain computer access to

²⁷⁴ *Id.*, at 526.

²⁷⁵ *Id.*

²⁷⁶ *Id.*

²⁷⁷ *Id.*

²⁷⁸ Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 *Calif. L. Rev.* 957, 969 (1989). See, also, Daniel J. Solove, *Conceptualizing Privacy*, *supra* note 9, at 1129.

²⁷⁹ Dean Pound, *supra* note 161, at 132.

²⁸⁰ Nevertheless, there are still some jurisdictions that still require actual trespass by the defendant See, e.g., *Pierson v. News Group Publications, Inc.*, 549 F. Supp. 635, 640 (S.D. Ga. 1982).

²⁸¹ *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).

THE CASE OF ON-LINE TERRITORIAL PRIVACY

a company's system.²⁸² Other courts have held that microscopic particles²⁸³ or smoke²⁸⁴ may give rise to trespass. And the California Supreme Court has intimated migrating intangibles (e.g., sound waves) may result in a trespass.²⁸⁵ More relevant to cyberspace's digital setting was the precedent upholding that electronic signals were sufficiently tangible to support a trespass cause of action.²⁸⁶ 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.*,²⁸⁷ the court has upheld that even a reaction up and down the line by a signal or a chain reaction is, in essence, electricity moving in interstate commerce.²⁸⁸ The Federal Power Commission court further argued, that no matter how small the quantity of the electromagnetic response, FPC jurisdiction 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.'²⁸⁹ Where previously the tort often required the tortfeasor's presence in the private space, the proposal allows the presence requirement to be fulfilled virtually, potentially expanding 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 by observing that an intrusion may be committed "by the use of the defendant's senses, with or without mechanical aids"²⁹⁰, used to oversee or overhear the plaintiff's private affairs, such as by looking into her upstairs windows with binoculars.²⁹¹ 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 his upstairs windows with binoculars are considered an invasion of her privacy.²⁹² 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

²⁸² *Thrifty-Tel, Inc. v. Bezenek*, supra note 213, *Id.*

²⁸³ *Bradley v. American Smelting and Refining Co.* (1985) 104 Wash.2d 677, 709 P.2d 782, 788-789.

²⁸⁴ *Ream v. Keen* (1992) 314 Or. 370, 838 P.2d 1073, 1075.

²⁸⁵ *Wilson v. Interlake Steel Co.*, 32 Cal.3d at pp. 233-234, 185 Cal.Rptr. 280, 649 P.2d 922.

²⁸⁶ *Thrifty-Tel, Inc. v. Bezenek*, supra note 213, 54 Cal.Rptr.2d 468 Cal.App.4.Dist., 1996. See, also, *CompuServe, Inc. v. Cyber Promotions, Inc.*, SUPRA NOTE 213, at 1021 (stating that electronic signals or messages provide sufficient contact to give rise to action for trespass to chattels).

²⁸⁷ See, supra note 135, *Id.*

²⁸⁸ *Id.*, at 458. See, also, Section 201 of the Federal Power Act owes its origin to the determination of this Court that a direct transfer of power from a utility in Rhode Island to a utility in Massachusetts is in interstate commerce, *Id.*, at 458. See *Public Utilities Comm'n v. Attleboro Steam & Electric Co.*, 273 U.S. 83, 47 S.Ct. 294, 71 L.Ed. 549 (1927). 'Part II (of the Act) is a direct result of Attleboro.' *United States v. Public Utilities Comm'n of California*, 345 U.S. 295, 311, 73 S.Ct. 706, 715, 97 L.Ed. 1020 (1953); *Connecticut Light & Power Co. v. FPC*, 324 U.S. 515, 65 S.Ct. 749, 89 L.Ed. 1150 (1945).

²⁸⁹ *Federal Power Commission v. Florida Power & Light Co.*, *Id.*, at 461. See, also, *Connecticut Light & Power Co. v. FPC*, 324 U.S. 515, 536, 65 S.Ct. 749, 759. See also *Pennsylvania Water & Power Co. v. FPC*, 343 U.S. 414, 72 S.Ct. 843, 96 L.Ed. 1042 (1952).

²⁹⁰ See, *Restatement (Second) of Torts*, supra note 14, § 652B, Comment (b).

²⁹¹ *Id.*

²⁹² 86 A.L.R.3d 374, supra note 16, § 3(A).

THE CASE OF ON-LINE TERRITORIAL PRIVACY

intrusions.²⁹³ Based on several updates and expansions of the Wiretap Act, the ECPA, in fact, expanded the protection of privacy against remote access from wire communications also to electronic communications from unauthorized interception, use and disclosure.²⁹⁴

Whenever taking a picture or taping someone may sometimes have captured the data subject's privacy inside her locale by importing its content 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 being there – we have intruded privacy by “uploading” that captured data to our locale. In comparison with the physical world, arguably, 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 a privacy subject matter.²⁹⁵ Cyberspace territorial privacy may arguably support an analogous proposition.

Alternatively, remote access can be made legitimate and thus has no intrinsic normative value, such as in the case of legitimate remote access from a private locale into a public one, where for instance, a naked woman is been observed with the use of binoculars and then identified while bathing at a public beach. In both types of activities, remote access is seen sufficient 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 to one locale. Multiple usage as either static presence or entry is, therefore, not unique to of network environments. It should, accordingly, 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. Privacy in these non-physical contexts can be generally understood in its familiar informational sense;²⁹⁶ it limits the ability of others to gain, disseminate, or use information about oneself.²⁹⁷ Like in the real world, in cyberspace, any gateway technology that would be seen as a public locale would avoid the risk of such illegal intrusion to whichever Internet user who will decide to enter it upon primer notice and choice to do so. Otherwise, for private locales

²⁹³ See, W. Page Keeton et al., *supra* note 15, § 117, at 854-55 (citing cases); See, *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).

²⁹⁴ 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. 18 U.S.C. § 2510(12) (1988), *supra* note 23, *Id.*

²⁹⁵ 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. App. 1996); *Clayton v. Richards*, 47 S.W.3d 149 (Tex. App. 2001).

²⁹⁶ See, e.g., *Jed Rubinfeld, The Right of Privacy*, *Harv. L. Rev.* 737 (1989), p. 740.

²⁹⁷ *Id.*

THE CASE OF ON-LINE TERRITORIAL PRIVACY

on-line, namely – private proprietary web sites that would be acknowledged as such, intrusion into a user’s private affairs would be seemed illegally intrusive.

2) *Non-physical distance: Reverse remote access*

Secondly, 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-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.²⁹⁸ 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 either her system and those of the linked system. Commentators sometimes refer to this process as employing "pull" technology: 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.²⁹⁹ 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.³⁰⁰ Thus, instead of users moving between locales remotely, the locales move between the users remotely, and information gathering is done, therefore, in the opposite order, but nevertheless remotely. As a result, allowing users to search for and retrieve of information stored in remote computers, as was also acknowledged as obiter

²⁹⁸ 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, also, I. Trotter Hardy, *The Ancient Doctrine of Trespass to Web Sites*, 1996 J. Online L. art. 7, §§ 10, 3.

²⁹⁹ 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) (9th Cir. filed June 22, 2000) (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"). The author provided comments on and signed this brief in support of Bidder's Edge, Inc. She received no compensation for this activity.

³⁰⁰ Storing a Web page in a cache constitutes copying. See, also, *MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993); *Advanced Computer Services v. MA Systems 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 & Policy Rev 25 (1994), p. 32 et al.

THE CASE OF ON-LINE TERRITORIAL PRIVACY

dictum by the *Reno v. ACLU* court.³⁰¹ Once the physical space-shifting requirement is inherently removed, remote access should be acknowledged in either direction. Only, as explained, in cyberspace access is made remotely but in the opposite direction; or 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.

Thirdly, it should be reminded 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. Eavesdropping, for instance, is thus allowed in a public locale. In *Nader v. General Motors*³⁰² 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.³⁰³ As comment c to § 652B of the Restatement explains, a person who moves about in a public locale has emerged from seclusion and thus opened herself up to observation by others.³⁰⁴ However, under certain circumstances, surveillance may be so 'overzealous' as to render it actionable.³⁰⁵ 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 real 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.³⁰⁶ Thus, legitimate observation should not reveal information that people wish to hide.³⁰⁷ The court in *Nader* established that "[a] person does not automatically make public everything he does merely by being in a public place."³⁰⁸ This conclusion should 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 is relatively cheap to achieve. Moreover, just like in the real world, such identifiers are words or symbols, which identify a specific person. Examples of identifiers in their meaning at the ECPA include Internet customer's name, address, social security number, credit card number, and proof of Internet connection obtained by Internet providers.³⁰⁹ As a result, observance and knowledge of a person's

³⁰¹ See, generally, *ACLU v. Reno*, supra note 61, at 834-36 (specifying remote information retrieval as one of the common methods of communication on the Internet).

³⁰² See, 255 N.E.2d 765 (N.Y. 1970).

³⁰³ *Id.*, at 771.

³⁰⁴ Upheld also in, *Dickson v. American Red Cross Nat. Headquarters*, 1997 WL 118415, N.D.Tex., 1997 (motion for summary judgment granted) referring to *K-Mart Corp. Store No. 7441 v. Trotti*, 677 S.W.2d 632, (Tex.App.--Houston [1st Dist.] 1984, writ ref'd n.r.e.).

³⁰⁵ *Dickson v. American Red Cross Nat. Headquarters*, *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 (1963)).

³⁰⁶ Marc Rotenberg, supra note 194, at 22

³⁰⁷ See also Restatement (Second) of Torts, supra note 14, at § 652B cmt. c ("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.").

³⁰⁸ *Nader v. General Motors*, at 771. ("[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."), *Id.* 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, Andrew Jay McClurg, supra note 14, at 1085-86 (1995).

³⁰⁹ 18 U.S.C.A., supra note 23, §§ 2510-2711. See, also, John M. Carroll, *Confidential Information Sources: Public & Private* 10 (2d ed. 1991), at 11-12. Raymond Nimmer mentions also specific

THE CASE OF ON-LINE TERRITORIAL PRIVACY

data identifiers - should remain a distinctive criterion in assessing privacy invasion on-line, even after territorial privacy is successfully integrated into cyberspace's privacy jurisprudence.

More particularly, on-line territorial privacy also should not alter the explicit premise in Dean Prosser's statement, adopted by the comments to the Restatement (Second) of Torts,³¹⁰ that 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.³¹¹ That legal framework should now also legitimize on-line non-identifiable data collection, for purposes such as for research on socio-economical trends or the development of statistics found in public locales, either through real time observance or 'sensor technology' or just occasional observance of user's behavior in on-line public locales.³¹²

Even more so, like in the real world, mere observation and/or legitimate data collecting should then be legalized notwithstanding if the collection of observed data was made for commercial use or not. The real world's law already admits such circumstances. For example, in the case of *Deteresa v. American Broadcasting Companies, Inc.*³¹³ Court upheld that under California law, a television producer's conduct in arranging for surreptitious videotaping of a woman in public view by camera person in public place, and in broadcasting only a five-second clip of tape, without broadcasting the woman's name or address, had insubstantial impact on privacy interests, and would not support the woman's intrusion into a seclusion privacy claim.³¹⁴ 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.³¹⁵ In other words, invasion of privacy by taking someone's picture, even for commercial use, is possible unless the picture tells the person's identity.³¹⁶ Such as when a photograph of her property has been used by the defendant in an advertisement, the plaintiff's identity must be apparent in the photograph.

individual's eligibility for government benefits; qualifications for employment; criminal records; draft records; real estate transactions; marriage; birth and death records; automobile registration; and tax liability. See, Raymond T. Nimmer, *The Law of Computer Technology* P 13.07 (2d ed. 1992), sec. 16.09.

³¹⁰ Page Keeton et al, *supra* note 15, s 117, at 855-56; Restatement (Second) of Torts, *supra* note 14, sec. 652B cmt. C.

³¹¹ Restatement (Second) of Torts, *Id.*, § 652B.

³¹² T. Nimmer, *supra* note 333, sec. 16.09. For such important web-based applications, such as telemedicine, data visualization, data-mining, and distance learning, see, e.g., CITRIS.Net projects, available at: <http://citris.ucdavis.edu/citrisnet.html>, or Continuous Output and Navigation Technology with Refinement On-Line (CONTROL) projects, available at: <http://control.cs.berkeley.edu:8000/control/>.

³¹³ See, 121 F.3d 460, C.A.9 (Cal.), 1997.

³¹⁴ *Id.*

³¹⁵ Restatement (Second) of Torts, *supra* note 14, § 652B.

³¹⁶ See, also, John M. Carroll, *supra* note 333, at. 11-12.

THE CASE OF ON-LINE TERRITORIAL PRIVACY

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 should 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 can be no 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.³¹⁷ This assumption of risk analysis is clearly discernible in *Gill v. Hearst Publishing Co.*,³¹⁸ a famous privacy case relied upon by Dean Prosser as support for his comments regarding absence of privacy in public locales.³¹⁹ The court grounded much of its reasoning in a kind of assumption of risk analysis, commenting that the plaintiffs were "in a pose voluntarily assumed in a public market place";³²⁰ 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";³²¹ that "[b]y their own voluntary action plaintiffs waived their right of privacy so far as this particular public pose was assumed";³²² and that the plaintiffs' right of privacy ceased by "their own voluntary assumption of this particular pose in a public place."³²³

In private locales, however, as the Restatement provision initially recognizes, to find true consent, the plaintiff must have full knowledge of the risk and voluntarily choose to encounter it. For an Internet customer to have reasonable expectation of privacy in her personal information under risk-analysis approach to Fourth Amendment:³²⁴ (1) data must not be knowingly exposed to others,³²⁵ and (2) Internet service provider's ability to access data must not constitute disclosure.³²⁶ That expectation of privacy, as explained, can be further applied to private locales. Moreover, like in the real world, when an on-line business is open to the public, a would-be entrant to the on-line locale in a given web site, at a reasonable time and in a reasonable manner, would have the implied

³¹⁷ Restatement (Second) of Torts, supra note 14, § 652B.

³¹⁸ See, 253 P.2d 441 (Cal. 1953).

³¹⁹ Prosser, supra note 9, at 391 n.81.

³²⁰ *Gill v. Hearst Publishing Co.*, supra note 342, at 444.

³²¹ *Id.*

³²² *Id.*

³²³ *Id.*

³²⁴ Assumption of risk is then 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 , supra note 14, sec. 496A.

³²⁵ U.S.C.A. Const.Amend. 4.

³²⁶ *Id.*, § 496C(1).

THE CASE OF ON-LINE TERRITORIAL PRIVACY

consent of the owner to be there, and so long as the person engages in no acts inconsistent with the purposes of the business or locale, there would be no trespass.³²⁷

Practically, should the courts choose this path based on on-line territorial privacy and the following construction of on-line locales, affected online service providers would be prohibited from freely disclosing their members' identities on the one hand, and relieved from the need to attest contractual consent in both types of locales and, arguably, should only be required to give adequate notice. As already acknowledged by the FTC, the notion that choice should be respected is almost universally accepted as a starting point for practical reasoning for privacy regulation.³²⁸ Such an invitation, however, presupposes that the conduct of would-be entrants will be in keeping with the nature of the locale.³²⁹ 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 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 built-in disclaimer into the website's locale or several locales, in the visitor's browser.³³⁰

Like with other precise legal fictions, the risk of over inclusive distinction between locales through the simple measurement of disclaimers therefore may entail a regulatory paradox. The more it continues to strive to grasp and define the essence of a legal proposition, such as the existence of on line spatiality, the farther we may get to promote its declared legal purposes. The court should initially confine itself to determining whether the 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.³³¹ In

³²⁷ 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).

³²⁸ Gavison, *supra* note 1, p. 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 (1998), available at <<http://www.ftc.gov/reports/privacy3/priv-23a.pdf>>, at 17.

³²⁹ See, *Mosher v. Cook United*, *supra* note 351, at 721; 25 Am. Jur. 2d Trespass, *supra* note 351, §48.

³³⁰ 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. Some 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 JavaScript Guide <<http://developer.netscape.com/docs/manuals/communicator/jsguide4/index.htm>>; An Exploration of Dynamic Documents, <http://home.netscape.com/assist/net_sites/pushpull.html>.

³³¹ Sharon K. Black, *supra* note 34, at 315 (applying this proposition to the information privacy category).

THE CASE OF ON-LINE TERRITORIAL PRIVACY

information privacy cases, in analogy, 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 break the lock, password or encryption.³³² A similar comparison could be made by courts to territorial privacy with users act to hide non-identifiable data upon entry to public locales. Upon entry to private locales, moreover, website owners may legitimize their collection activities, upon notice, clarifying that the web site owner collecting such data may override identity concealment measurements used by would-be entrants to such locales.³³³

b. Proportional cost of control

Recognition of distinct locales also requires that the cost of control should match the particular functions on the whole sub segment of types of locations, namely private and public. Based on information privacy analysis, the legal problem has been likely to be detection of "trespasses" or the unauthorized use of an informational work.³³⁴ As noted earlier, practical problems exist with policing very long borders of real property, but they seem to pale beside the problem of detecting "trespass" activities like unauthorized copying or uses of informational works.³³⁵ If these costs are excessive in cyberspace, they might argue against a private-property regime because such a regime would not be "worth it".³³⁶

Based on an acknowledgment of territorial privacy, however, there should be a difference between control over content use as assessed through information privacy protection, and control over access. As explained, 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.³³⁷ 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.³³⁸ A similar presumption to that of trespass to land, however, exists in case of privacy invasion according to the tort of intrusion upon seclusion. Invasion is intrinsically foul, even with no harm, as 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."³³⁹ In other words, an intrusion on privacy is intrinsically harmful because it is defined as that which

³³² *Id.*, at 315 and Fn. 195 & accompanying text.

³³³ *Id.*

³³⁴ Trotter Hardy, *supra* note 43, at 247.

³³⁵ *Id.*

³³⁶ *Id.*

³³⁷ For the context of trespass – See, Restatement (Second) of Torts, *supra* note 14, § 218 cmt. e (1965). See, also, Page Keeton et al, *supra* note 15, at 67 (W. Page Keeton ed., 5th ed. 1984) (outlining the historical cause of action in trespass).

³³⁸ *Id.*

³³⁹ Gavison, *supra* note 1, at 426 n. 18.

THE CASE OF ON-LINE TERRITORIAL PRIVACY

injures social personality.³⁴⁰ 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.³⁴¹

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.³⁴² With this lowered standard of proof of infringing behavior, and by analogy, 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.³⁴³ Consequently, privacy norms against intrusion could be more upheld in cyberspace, especially given the fact that surveillance technology only makes illegal collection of information easier and cheaper to attain.

Notably, in tort law, full level of control by owners is only required in private locales. Alternatively, any lack of sufficient level of actual control does not negate the concept of spatiality at large, but rather only the possibility that such locale may be constituted as a private one. Like in real world jurisprudence, virtual spatiality framed as public, may still be upheld.³⁴⁴ In such cases, the legal standard for spatiality could still constitute an on-line public locale, just like in the real world.

3. *The presumption has to be either*

- a) *Conclusive, or*
- b) *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 actually a substantive rule of law.³⁴⁵ 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.³⁴⁶ Accordingly, dogmatic fictions should never be used, as the historic fictions were used in the past, to change the law, but only for the purpose of classifying

³⁴⁰ *Id.*

³⁴¹ Robert C. Post, *supra* note 302, at 964; Gavison, *supra* note 1, at 425-40.

³⁴² Robert C. Post, *Id.*

³⁴³ O'Rourke, Property Rights and Competition, *supra* note 43, at 587; For the difference between "damage" torts and "interference" torts, see Robert Post, *supra* note 302, at p. 964 and Fn. 42 & accompanying text.

³⁴⁴ See, e.g., *See Shulman v. Group W Productions, Inc.*, 18 Cal.4th 200, 232 (1998) (holding that filming a rescue attempt at an accident scene, 50-feet down an embankment of an interstate highway, was not an invasion of plaintiff's privacy); upheld also in *Salazar v. Golden State Warriors*, 2000 WL 246586, N.D.Cal.,2000. There, the California Supreme Court has 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.

³⁴⁵ 9 J. Wigmore, *supra* note 239, at § 2492 (3d ed. 1940); C. McCormick, *Evidence* § 342 at 804 (2d ed. 1972).

³⁴⁶ J. Gray, *The nature and sources of law* 30-37 (1921).

THE CASE OF ON-LINE TERRITORIAL PRIVACY

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 applicative and a direct and inevitable continuation of locales in the real world. One should, consequently, be able to state the real doctrine for which they stand.³⁴⁷ Ultimately, the legal necessity for an adequate technical vocabulary makes it desirable that well-founded fictions such as, arguably, on-line locales – converted into legal truth, would be picked with appropriate judicial discretion.³⁴⁸

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.³⁴⁹ That is also why the other type of presumption, namely – the rebuttable presumption should not be preferred in the construction of on-line locales. Rebuttable presumptions are instead, 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.³⁵⁰ As explained, 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 dissimilarity, which is subtle but not unreal. As unreal constructions, on-line locales are not a conclusion which the [trier of fact] is *permitted*, but not compelled, to draw from the facts.³⁵¹ Instead, as real presumptions, also called presumptions of law, on line locales should be made an inference, through which the law directs the [trier of fact] to functionally draw if it finds a given set of justifications, as explained. 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,³⁵² in pre-print archives of articles enabling scientists to share the latest learning in their fields,³⁵³ web resources on the poster's favorite topic,³⁵⁴ etc.

³⁴⁷ *Id.*, at 37.

³⁴⁸ L. Fuller, *supra* note 131, at 23.

³⁴⁹ C. McCormick, Evidence § 345 at 822-823 (2d ed. 1972).

³⁵⁰ Olin Guy Wellborn III, *The rules of evidence: Cases and materials* (West, 2000), p. 553.

³⁵¹ *Bray v. United States*, 113 U.S.App.D.C. 136, 140, 306 F.2d 743, 747 (1962).

³⁵² See, e.g., Slashdot, at <http://slashdot.org>

³⁵³ See Los Alamos Physics Preprint Server, at <http://www.arxiv.org>

³⁵⁴ See, e.g., Archinect: Architectural and Urban Planning Sites, at <http://www.archinect.com>

VI.
SUMMARY AND CONCLUSIONS

Thus far, cyberspace has not been left with a public sphere and locales, nor has a balanced privacy policy been established. Instead, only a *private*, and too wide, privacy legal rule has been adopted. Thus, database protection against the various forms of information collection, but particularly registration data that is collected upon initial entry to databases, is arguably an overly generalized 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 continuation to previous jurisprudential developments, privacy should continue to be valued instrumentally. Courts may then be required to differentiate and identify private locales and then fence them out from public ones. Thus, a legal fiction of on-line locales should now be constructed for cyberspace's overall privacy policy.³⁵⁵

In public locales, privacy protection should instead 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, with regard to databases, much information collection and use, occurs in what would otherwise be considered public, and as argued, many parts of cyberspace may well be considered public locales. In balance, adaptation of ECPA's "in storage" definition in Title II, primarily, to territorial privacy would then enhance the protection given to information collected in private locales.

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

In cyberspace, nonetheless, the U.S. federal government and primarily the FTC's privacy policy, in fact, still encourages the withdrawal of law as a balancing constraint, as seen with the FTC's stance toward online privacy, which emphasizes technological and market self-regulation jointly, for the adoption of privacy policies. As shown, however, technology alone thus far, has failed to provide protection comparable to that, which could be provided with the intervention of law. Technology, thus far, has been incapable of establishing a comprehensive boundary solution only by itself.

³⁵⁵ See e.g., Andrew L. Shapiro, *supra* note 42 (in justification of the 1st Amendment "public forum" doctrine); David J. Goldstone, *supra* note 43, at 3 (same).

THE CASE OF ON-LINE TERRITORIAL PRIVACY

A legal fiction of on-line locales, in balance, can arguably be easily 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, as explained, can be further applied to private locales. Moreover, like in the real world, when an on-line business is open to the public, a would-be entrant to the on-line locale in a given web site, at a reasonable time and in a reasonable manner, would have the implied consent of the owner to be there, and so long as the person engages in no acts inconsistent with the purposes of the business or locale, there would be no illegal intrusion.

More particularly, territorial privacy on-line should also not alter the explicit premise in Prosser's statement, adopted by the comments to the Restatement (Second) of Torts,³⁵⁶ that there is no difference between merely observing a person in a public locale and taking her photograph. Thus, in correspondence with 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. As shown, that legal framework should now also legitimize on-line non-identifiable data collection, for purposes such as for research on trends or the development of statistics in public locales, either through real time observance sensor-based technology or just occasional observance of user's behavior in public locales on-line.

Even more so, just like in the real world, mere observation and/or legitimate data collecting in on-line locales should then be seen legal notwithstanding if the collection of observed data was made for commercial use or not. The real 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 whichever types of information, namely, transactional, registration and clickstream data, that would be abided to by would-be entrants; in public locales, however, observance should be freely allowed, as long as a notice of the public locale is brought forth, but then be solely restricted to the collection of non-identifiable registration and clickstream data.

In balance, legitimate observation should not reveal data identifiers that people wish to hide. Like in the real world, such identifiers are words or symbols, which identify a specific person. Examples of identifiers in their meaning at the Electronic Communications Privacy Act include Internet customer's name, address, social security number, credit card number or proof of Internet connection obtained by Internet providers. As a result, observance and knowledge of a person's data identifiers - should remain a distinctive criterion in assessing privacy invasion on-line, even after territorial privacy is successfully integrated into cyberspace's privacy jurisprudence. This conclusion should still be held valid when entry is made non-physically, as in cyberspace; and any recognition of remote entry should be evaluated within this normative framework.

³⁵⁶ Page Keeton et al, supra note 15, s 117, at 855-56; Restatement (Second) of Torts , supra note 14, sec. 652B cmt. c.

THE CASE OF ON-LINE TERRITORIAL PRIVACY

Moreover, any lack of sufficient level of actual control should not negate the concept of spatiality at large, but rather only 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 real 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 real presumptions, also called presumptions of law, on line locales should be made an inference, through which the law directs the [trier of fact] to functionally draw if it finds a given set of justifications, as explained. 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.

Like in the real world, ultimately, on-line public locales will finally legitimize the supervision of public health, a territorially based collection of taxes, the enforcement of the criminal and First Amendment policies and even the possible use of copyrighted information distributed through the public sphere. That is, either if ownership of public locales is public, private or a combination of the two.

END OF DOCUMENT