University of California, at Berkeley School of Law (Boalt Hall)

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

By: Daniel Benoliel**

A. Territorial Privacy: The normative framework

Privacy is 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 found but also legally constructed. Overall, privacy can be divided into four categories.[2] The first is bodily privacy, which addressed 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 freely to communicate among peers. It covers the various interests of individuals in communicating among them using various forms of communications. The third is information privacy, which concerns the control and handling of personal data.[4] 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[5] and Roe v. Wade.[6]

The fourth, and the focal point of this synopsis, is territorial privacy, which involves setting limits boundaries on intrusion into an explicit space or area. Turning our focus from disruptions to the practices they disrupt, we often refer to aspects of these practices

---

** J.S.D. candidate, UC Berkeley, School of Law (Boalt Hall). This is a synopsis of a study that 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). For their most helpful comments and support, I am indebted to Pamela Samuelson, Mark Lemley, Dan Hunter, the Chief Scientist of CITRIS - James Demmel and David Wagner. Any inaccuracies would be my responsibility. For further questions or comments, please email me at: Daniel_b@boalthall.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).

2 See, e.g., Ruth Gavison, ibid, 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 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).

5 381 U.S. 479 (1965)

6 410 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 he "individual interest in avoiding disclosure of personal matters", with the individual's "independence in making certain kinds of important decisions". Id. at 599-600.

as "private matters." In other words, we say that certain things, places, and affairs are "private."[7] Initially, Courts designated two classes of excluded areas: "private" areas, as a home,[8] or a reserved hotel room, [9] in which the individual can expect to be free from governmental intrusion[10] and "non-private" areas, in which the individual does not have a recognized expectation of privacy.[11] The designation of an area as "private" protected the personal information located there from governmental seizure. The Restatement (Second) of Torts most notably incorporated these views in the comments to section 652B, [12] which defines the tort of intrusion.[13] Thus, Courts held almost uniformly that the tort of intrusion couldn't occur in a public place or in a place that may be viewed from a public place.[14] On the public street, or in any other public place, the plaintiff has no legal right to be alone;[15] the circumstances themselves in such cases are not secluded; [16] and it is no invasion of her privacy to do no more than follow her about and watch her there.[17]

Thus 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.[18] Instead, only a vision of information privacy or data protection has, thus far, been embodied constituting privacy guidelines issued in 1980 by the Organization for Economic Cooperation and Development. These guidelines outline a set of Fair

---

7 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.

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

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

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

11 Id.

12 For an exception recognizing a cause of action of privacy intrusion in the public sphere, see, Restatement (Second) of Torts, supra note 4, § 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) (upholding "public privacy" paradigm and a tortuous cause of action), pp. 1045-1055.

13 See, e.g., Restatement (Second) of Torts, § 652B cmt. c.

14 See, also W. Page Keeton et al., Prosser & Keeton on the Law of Torts (5th ed. 1984), § 117, at 855-56; William L. Prosser, supra note 7, p. 391-92; Andrew Jay Mcclurg, supra note 12, 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.).

15 W. Page Keeton et al., supra note 14, at 855 & n.68; 86 A.L.R.3d 374, Taking Unauthorized Photographs as Invasion of Privacy (ed. Phillip E. Hassman), § 2.

16 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.).

17 W. Page Keeton et al., supra note 14, at 855 & n.68; 86 A.L.R.3d 374, Taking Unauthorized Photographs as Invasion of Privacy (ed. Phillip E. Hassman), § 2.

18 See, discussion at Part B.1, herein.

Information Practices (FIPs) based on eight principles: [19] collection limitation, data quality, purpose specification, use limitation, transparency of information collection practices, security of stored data, individual participation, and accountability.[20] Strictly adhering to the category information privacy, Congress also passed the Electronic Communications Privacy Act (ECPA) of 1986[21] updated the Wiretap Act of 1968. [22] Specifically, it expanded the coverage of the Wiretap Act by adding information or database privacy protection through Title 1,[23] addressing the unauthorized interception of computer databases or electronic communications while "in transit"; and Title 2,[24] addressing the unauthorized acquisition of electronic communications while "in storage". 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 cyberspace, currently, there are two basic ways to collect such personal information. The first, by directly collecting information from users (registration and transactional data); [25] Registration data is collected by those websites that request users to log in to access parts of the website. Transactional data is gleaned by websites engaging in business with users, such as selling merchandise or services.[26] 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 most popular. [27]

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 privacy category to include both possible public and private on-line locales, while overly protecting the latter. On 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. That is, while balancing it with the real world privacy law rationales of protecting legitimate observance and non-identifiable data collection in public locales either directly or indirectly by websites. Notably, with regard to databases, much information collection and use occurs in what would otherwise

---

19 See U.S. Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace (2000).

20 See Organisation 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). 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); Julie E. Cohen, DRM and privacy, 18 Berkeley Tech. & L.J. 575.

21 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).

22 18 U.S.C. §§ 2510-21 and 2701-10

23 Id, §§ 2510-2521 (1988).

24 Id.

25 Daniel J. Solove, Privacy and power: Computer databases and metaphors for information privacy, 53 Stan. L. Rev. 1393, p. 1411.

26 *Id*,

27 *Id*.

be considered public, and indeed, many parts of cyberspace may well be considered public locales. [28] 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 locale may avoid over fragmentation of regulative realms.[29] In fact, private and public locales could coexist on the Internet, just as they do in the physical world.[30] Courts may then be required to differentiate and identify private spheres and then fence them out from public ones. Thus far, cyberspace was not left with a public sphere and locales, nor a balanced privacy policy was established. Instead, only a *private*, and too wide, privacy legal rule was adopted. In continuation to previous jurisprudential development, privacy should continue to be valued instrumentally.[31] Thus, a legal fiction of territorial locales should now be constructed for cyberspace's overall privacy policy.

B. Constructing locales as a legal fiction

The authority of courts to serve process and enforce orders ordinarily stops at territorial boundaries, with the exception of long arms. In the Anglo-American legal system standing, moreover, is conferred on the injured; while "injury" has been orthodoxy construed in terms that assume plaintiff's presence at the scene of the complained of wrong. In fact, areal analysis, which refers to localist boundary theory, tends to place talismanic weight on physical location and distance as its core concern.[32] An individual physically present in an area has a cognizable interest in its locale;[33] just as governments

---

28 Daniel J. Solove, supra note 25, at 1433.

29 Julie E. Cohen, supra note 20, at 592 (suggesting that computers, for instance, sit at the center of such privacy zones, regardless of where in physical space it happens to be located).

30 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).

31 See, also, Daniel J. Solove, supra note 7, at 1144-1145; Julie C. Inness, Privacy, Intimacy, and Isolation 3 (1992), 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.

32 Daniel A. Farber, Stretching The Margins: The Geographic Nexus in Environmental Law, Stan. L. Rev. 1247 (1996), p. 1270; 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 Rekkan (Eds.), p. 53.

33 J.R.V. Prescott, Political geography (Methuen & Co. Ltd, 1972), pp. 54, 61-74; Suzanne Lalonde, Determining boundaries in a conflicted world (McGill-Queen's University Press, 2002), p. 8 and mentioned sources; J.R.V. Prescot, Political frontiers and boundaries (London: Unwin Hyman, 1987), p. 36; 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; T. Cresswell, In place, out of place: Geography, ideology and transgression (University of Minnesota Press, 1996), p. 149. In the physical world, with no appropriate analogy to network environments, Borderland is then 'the transition zone within which the boundary lies'. J.R.V. Prescot, pp. 13-14, *Id.*

have a legitimate interest in harms that are physically present within their separated territories.[34]

1. First heterogeneity: Physical presence

First, applying localist boundary theory to cyberspace is confronted with the physical world's notion that locales most be physical. Thus, although data have been traveling on wires and through the airwaves for centuries, the television, the telegraph, or the telephone are not "places" within which people travel.[35] 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.[36] There were computer networks before the Internet that similarly relied on telephonic exchange of data.[37] 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.[38] 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.[39] To be capable of appropriation an island territory must apparently present at high tide a surface of land clear of the water, which is large enough to be habitable in practice.[40] This pragmatic notion of placeless seems to have led some public international law scholars all the way to insist that the

---

34 See, Daniel A. Farber, supra note 32, at 1270.

35 Andrew L. Shapiro, The Control Revolution: How the Internet Is Putting Individuals in Charge and Changing the World We Know (1999) (cyberspace is not a real place but just a medium that we may control), pp. 710-712; Andrew L. Shapiro, The Disappearance of Cyberspace and the Rise of Code, 8 Seton Hall Const. L.J. 703 (1998), p. 709 and see Fn. 21 & accompanying text; Timothy Wu, When Law & the Internet First Met, 3 Green Bag 2d 171 (1999-2000).

36 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).

37 For a discussion of the prevalence of private "bulletin board systems" in the late 1980s and early 1990s, see, e.g., Debra B. Burke, id.

38 Andrew L. Shapiro, supra note 35 (for the legal perspective), pp. 710-712; Timothy Wu, When Law & the Internet First Met, 3 Green Bag 2d 171 (1999-2000) (same). See, also, Edward W. Soja, Postmodern Geographies: The Reassertion of Space in Critical Social Theory (1989) ((For the political geography perspective).

39 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), p. 22, referring to Laurent Lucchini & Michel Voelckel, Droit de la mer, vol. I (Paris, Pedone, 1990), p. 331.

40 International Court of Justice, 1953, pp. 49, 53.

islands must also be shown on geographical maps.[41] Nevertheless, a dopting a not less pragmatic approach, the Anglo-American legal system, has consistently acknowledged non-physical forms of spatiality, and in various constitutional contexts. In seminal First Amendment cases such as Perry[42] and Cornelius, [43] 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."[44] In another context, in United States v. Grace,[45] the Court divided the Supreme Court grounds into perimeter sidewalks and interior grounds,[46] relying on the sidewalks' functional continuity with the adjoining streets[47] and indistinguishability from other public walkways. [48] 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. Recognition of a fictitious 'place' was instead made functional. Any remaining doubts that such a functionally defined place could qualify as a public forum were dispelled in Rosenberger,[49] where the Court characterized the university's student activity funding system as "open[ing] a limited forum"[50] 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".[51] 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 public fora that do not always have to be physical gathering places.[52] Whenever such functionally based analysis entails (and only then), there must be no inherent objection to why shouldn't our legal system fictitiously expand the notion of locales other virtual realms, such as cyberspace.

---

41 See Monique Chemillier-Gendreau, supra note 39, at 22, referring to Gilbert Gidel, La mer territoriale at la zone contig_e, (1934) Recueil des Courts de l'Academie de Droit International, II, vol. 48, pp. 137-278.

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

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

44 Id. at 801.

45 461 U.S. 171 (1983).

46 Id. at 179-80.

47 Id. at 180.

48 Id. at 179.

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

50 Id. at 829. The Court uses the term "limited" or "designated" forum to denote a forum that, at least for a class of speech that may be limited by speaker and/or subject-matter, will be treated as a "public forum." See id.; ISKCON, 505 U.S. 672, 678 (1992) ("The second category of public property is the designated public forum, whether of a limited or unlimited character-- property that the State has opened for expressive activity by part or all of the public. Regulation of such property is subject to the same limitations as that governing a traditional public forum.") (citations omitted). See infra Part II.A.2.

51 515 U.S. at 830.

52 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).

2. Second heterogeneity: Distance

A second weakness of the homogenous definition of space is threatened by heterogeneity due to the existence of distance and its influence on entry preferences on individuals.[53] 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.[54] Nevertheless, in comparing non-material electronic access to material 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. For start, the requirement of actual trespass was largely abandoned with the tort of privacy intrusion.[55] 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,[56] 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 company's system.[57] Other courts have held that microscopic particles[58] or smoke [59] may give rise to trespass. And the California Supreme Court has intimated migrating intangibles (e.g., sound waves) may result in a trespass.[60] More relevant to cyberspace's setting was the precedent upholding that electronic signals were sufficiently tangible to support a trespass cause of action.[61] 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.,[62] 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.[63] In what is a

---

53 J.R.V. Prescott, supra note 33, at 54, 56-61; Suzanne Lalonde, Determining boundaries in a conflicted world (McGill-Queen's University Press, 2002), p. 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.

54 J.R.V. Prescott, supra note 33, at 54, 56-61; Suzanne Lalonde, at 8, *Id.* and mentioned sources; L.K.D Kristof, supra note 33, at 127.

55 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).

56 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).

57 Thrifty-Tel, Inc. v. Bezenek, 54 Cal.Rptr.2d 468 Cal.App.4.Dist., 1996

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

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

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

61 Thrifty-Tel, Inc. v. Bezenek, 54 Cal.Rptr.2d 468 Cal.App.4.Dist., 1996. see, also, CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (stating that electronic signals or messages provide sufficient contact to give rise to action for trespass to chattels).

62 92 S.Ct. 637 U.S. Fla. 1972. Decided Jan. 12, 1972; 405 U.S. 948, 92 S.Ct. 929 (Reversed and remanded).

63 Id, p. 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

natural proxy to cyberspace's communication, 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.'[64] 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 spaces by 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, to oversee or overhear the plaintiff's private affairs, as by looking into his upstairs windows with binoculars...".[65] Thus, when a picture is taken of a plaintiff while he or she is in the privacy of his or 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 his privacy.[66] Overall, most courts today do not require the physical penetration of private locales as an ingredient of spatial invasion of privacy. Wiretapping, bugging rooms with microphones, and peering into windows have all been held to constitute actionable intrusions even without physical entry.[67] Nevertheless, because surreptitious recording devices generally require that some sort of technical trespass to land or chattels be committed, through either their installation or introduction, they are more properly viewed as belonging to that category of intrusions involving a trespass.[68]

Moreover, whenever taking a picture or taping someone may sometimes captured the data subject's privacy inside his or 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 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 (but not all) analogous physical environments. For start, such is the case with surveillance into a private sphere or locale

---

interstate commerce (p. 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).

64 Ibid, p. 461. See, also, Connecticut Ligh & 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).

65 See, Restatement (Second) of Torts, § 652B, Comment (b).

66 86 A.L.R.3d 374, Taking Unauthorized Photographs as Invasion of Privacy (ed. Phillip E. Hassman), § 3(A)

67 See, Prosser & Keeton on Torts, supra note 14, § 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).

68 See, e.g., Shulman v. Group W Prod., Inc., 955 P.2d 469, 492 (Cal. 1998) (analogizing mechanical recording devices to an "unannounced second auditor" in concluding that a reporter's act of attaching a microphone to a paramedic might constitute an actionable intrusion upon seclusion), id.

from a public sphere or locale, where invasion of privacy is done by technical surveillance that allows identification of the privacy subject matter. 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 sphere into a public sphere, 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 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;[69] it limits the ability of others to gain, disseminate, or use information about oneself.[70] Like in the real world, in network environments, 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 choice to do so. Otherwise, for private locales 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.

Secondly, and more specifically, this 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 third category of space shifting should be assumed in network environments. 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.[71] 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 his or her own 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

---

69 Jed Rubenfeld, The Right of Privacy, Harv. L. Rev. 737 (1989), p. 740.

70 *Id*.

71 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 assumptions apply 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, 13.

be interested in it.[72] In both cases, space shifting is then seen theologically pleasing. 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.[73] 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 by the Reno v. ACLU court.[74] Once the physical space shifting requirement is inherently removed, remote access can be acknowledged in either direction. Only, as explained, in network environments access is done remotely but in the opposite direction, or otherwise, the locale or some electronic parts of it visits us upon earlier request.

C. Why don't we have distinctive locales in cyberspace?

The inclination to either ignore differentiation between locales on-line nevertheless seems to be based on largely accepted deformations of cyberspace's architecture, in comparison to physical world cartography. 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, imbeds a different structure. In the latter, apart from the net's "public roads" or backbone transit infrastructure, which is regulated according to public law and Antitrust, the present default rule contains a mosaic of private allotments – namely, neighboring proprietary web sites. In fact, cyberspace was left without publicly (but even privately) owned 'squares', 'sidewalks' or even 'shopping malls' and thus neither a public sphere nor balanced privacy policy was so far established. Instead, only a private privacy legal rule was adopted and too widely so. The construction of a legal fiction of private and public locales could ultimately solve this anomaly and reestablish the inner balance of privacy protection for cyberspace.
END OF DOCUMENT

---

72 Jerry Kang, Cyber-Race, 113 Harv. L. Rev. 1130, 1148 (2000) ("'Push' communications arrive at the receiver without any special effort on the part of the receiver to obtain that particular communication item.... By contrast, 'pull' communications require more focused effort by the receiver to retrieve particular information. Surfing the Web is a common example of pull technology."); see also Brief of Amici Curiae Law Professors at 7, 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) [[[hereinafter Brief of Amici Curiae Law Professors] (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.

73 Storing a Web page in a cache constitutes the making of a "copy"-as it well might under the view of such cases as MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511 (9th Cir. 1993) and Advanced Computer Services v. MA Systems Corp., 845 F.Supp. 356 (E.D. Va. 1994), holding that transitory fixation in RAM constitutes copying for purposes of the Copyright Act. Not all uses deliver information through copying. Some deliver information in digital streams without permanent fixation at all, such as "music on demand" services, which charge for access or immediate performance. See, 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.

74 See, generally, ACLU v. Reno, 929 F. Supp. at 834-36 (surveying common methods of communication on the Internet, including remote information retrieval).