

2007

Clouds, Cameras, and Computers: The First Amendment and Networked Public Places

Timothy Zick

William & Mary Law School, tzick@wm.edu

Repository Citation

Zick, Timothy, "Clouds, Cameras, and Computers: The First Amendment and Networked Public Places" (2007). *Faculty Publications*. 96.

<https://scholarship.law.wm.edu/facpubs/96>

Copyright c 2007 by the authors. This article is brought to you by the William & Mary Law School Scholarship Repository.

<https://scholarship.law.wm.edu/facpubs>

Florida Law Review

Founded 1948

Formerly
University of Florida Law Review

VOLUME 59

JANUARY 2007

NUMBER 1

CLOUDS, CAMERAS, AND COMPUTERS: THE FIRST AMENDMENT AND NETWORKED PUBLIC PLACES

*Timothy Zick**

I.	INTRODUCTION	2
II.	FROM MATERIAL TO NETWORKED PUBLIC PLACES	6
	A. <i>Speech in Material Public Places</i>	6
	B. <i>The Networking of Public Places</i>	10
	1. <i>Wireless Clouds—"Muni WiFi"</i>	11
	2. <i>Surveillance Square</i>	14
	3. <i>Pervasive Computing and</i> <i>Mobile Technologies</i>	18
III.	FREEDOM OF EXPRESSION IN NETWORKED PUBLIC PLACES	22
	A. <i>Property: The Legal Status of Wireless Clouds</i>	22
	B. <i>Public "Captivity"</i>	26
	C. <i>Protection: Dangerous, Offensive, and Harmful</i> <i>Speech Activity</i>	31
	D. <i>Protest: Assembly, Association, and Anticipatory</i> <i>Conformity</i>	36
	E. <i>Privacy: Identity, Thought, and Compulsory Speech</i>	38
	F. <i>Press: "Citizen-Journalists" and Disclosures of</i> <i>Private Information</i>	42
IV.	NETWORKED PUBLIC PLACES AND DEMOCRATIC VALUES	47
	A. <i>Public Places and the Public Sphere</i>	48

* Associate Professor of Law, St. John's University School of Law. I would like to thank Paige Price for her support and encouragement. I would also like to thank the editors of the *Florida Law Review* for their diligent work.

B. <i>The Democratic Functions of Public Places</i>	50
1. Place and Identity	50
2. Place and Self-Governance	52
3. Place and Transparency	53
C. <i>The Networked Public Citizen</i>	54
1. Populated Places and the Public Digital Divide	54
2. The People—Disconnected	56
3. The Purification of Public Places	58
D. <i>Retaining the Civic Character of Public Places—Some Modest Proposals</i>	62
1. Ownership and Access	62
2. Regulatory Transparency	64
3. Protest Tactics, “Sousveillance,” and Civil Disobedience	65
4. Laws, Norms, and Architectures	67
V. CONCLUSION	68

I. INTRODUCTION

It seems to be a common assumption that physical places like parks, sidewalks, and public squares, and “cyber-places” like the Web, constitute separate locations of communication. In reality, however, the intersection and collision of these two spaces is imminent. In some respects it has already occurred. Entire cities and counties are erecting wireless “clouds” that will bring the Internet to vast public spaces.¹ Technologies of surveillance continue to proliferate. What one does and says in public places is increasingly subject to surveillance by means of a combination of hand-held devices and official surveillance tools like closed circuit television cameras (CCTV).² There may soon be a continuous, running record of most public activities. People in public places are also carrying

1. See Sewell Chan, *After Delays, Wireless Web Comes to Parks*, N.Y. TIMES, July 6, 2006, at B1 (reporting plans to provide free wireless access in many New York City parks). The Former Yugoslav Republic of Macedonia plans to become the first country to go completely wireless. See Nicholas Wood, *Macedonia Dreams of One Nation, Wireless*, N.Y. TIMES, Apr. 3, 2006, at A9. Rhode Island has plans to become the first American state to go wireless from border to border. See Jesse Noyes, *R.I. Planning to Go WiFi*, BOSTON HERALD, Apr. 29, 2006, at 19. For a summary of local government wireless activity to date, see Sharon E. Gillett, *Municipal Wireless Broadband: Hype or Harbinger?*, 79 S. CAL. L. REV. 561, 565-81 (2006).

2. See Aimee Jodoi Lum, Comment, *Don’t Smile, Your Image Has Just Been Recorded on a Camera Phone: The Need for Privacy in the Public Sphere*, 27 U. HAW. L. REV. 377, 396-404 (2005) (discussing privacy and public voyeurism laws). Closed circuit television (CCTV) systems typically involve a dedicated communications link between cameras and monitors. This permits cameras to be viewed and operated from a control room. See *CCTV: Constant Cameras Track Violators*, NAT’L INST. OF JUSTICE, July 2003, at 16 (explaining CCTV technology).

and wearing ever more sophisticated computing devices. Pervasive personal computing is mobilizing communication and affecting public interaction in ways we are only now beginning to appreciate. Among other things, it is blurring the line between private and public communication. Anyone who has ever been stuck in traffic behind a car in which a pornographic DVD is being displayed has glimpsed this phenomenon. Like it or not, the era of “drive-by pornography” is now upon us.³

Technology is altering the fundamental character of public places. Increasingly, when we are in public, we occupy “networked” places.⁴ Some scholars have already noted the significant Fourth Amendment privacy concerns raised by the networking of public places.⁵ These concerns will be exacerbated as the technologies of communication and surveillance become more widespread and more sophisticated. The networking of public places will also give rise to a host of less-commented upon free speech issues.⁶ Place is a critical component of expressive activity.⁷ The transformation of material public places into networked ones will fundamentally change what it means to speak, petition, associate, and exercise press rights in public.

This Article provides a comprehensive assessment of the First Amendment issues related to the networking of public places. The changes brought about by the networking of public places will affect a number of First Amendment doctrines and principles. This Article considers six basic

3. See Rachel Leonard, ‘Dirty Driving’ Sore Spot for Legislators, Officers, SPARTANBURG HERALD-J., Jan. 12, 2006, <http://goupstate.com/apps/pbcs.dll/article?AID=/20060112/NEWS/601120372/1051/NEWS01%22>.

4. See Jerry Kang & Dana Cuff, *Pervasive Computing: Embedding the Public Square*, 62 WASH. & LEE L. REV. 93, 94 (2005) (“If the line between cyberspace and real space has grown increasingly difficult to draw, it may soon become impossible.”). The term “networked” has been applied to spaces in other contexts. Writing specifically about cyberspace, for example, Julie Cohen has argued that we are witnessing the rise of a new type of social space, which she calls “networked space.” Julie E. Cohen, *Cyberspace as/and Space*, 117 COLUM. L. REV. (forthcoming 2007), available at <http://www.lawgeorgetown.edu/faculty/jec/cyberspace.pdf>. This Article adapts the concept to emphasize the effect new technologies, including but not limited to the Internet, will have on public places and public expression.

5. See JEFFREY ROSEN, *THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA* (2000); Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World That Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1426-33 (2004); Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213 (2002).

6. For a thoughtful discussion regarding the effects that monitoring urban public space may have on anonymity, see Marc Jonathan Blitz, *The Dangers of Fighting Terrorism With Technocommunitarianism: Constitutional Protections of Free Expression, Exploration, and Unmonitored Activity in Urban Spaces*, 32 FORDHAM URB. L.J. 677, 702-19 (2005).

7. See Timothy Zick, *Speech and Spatial Tactics*, 84 TEX. L. REV. 581, 617-25 (2006) (describing the importance of public places to expressive rights) [hereinafter Zick, *Speech and Spatial Tactics*].

categories or clusters of speech issues raised by the networking of public places: property or public forum, public captivity, protection (from harmful speech), public protest, privacy (in terms of both identity and thought), and press.

Having cities and other governmental entities, rather than private interests, provide public wireless Internet connections raises questions about ownership, control, access, and neutrality. Are these public wireless networks just another public utility? Are they speech forums? Will governments, or their private partners, be able to filter public Web access? Is there a constitutional *right* to public connectivity and access in the same sense that there is a right to speak and assemble on the streets? Will governments, or their state-actor private partners, have unfettered access to information about public network users?

Public “captivity” will also become a larger concern. As the drive-by pornography example shows, the networking of public places will expose audiences to speech in public that has to this point been either entirely private or effectively segregated in material places. Sexually explicit content and ubiquitous advertising will be more prevalent in networked places. Citizens will carry this content with them into the networked public square. We will all potentially be more “captive” in networked public places—on buses, in subway cars, in parks and government buildings—to speech that we have generally been able to avoid in material public places.⁸ To what extent can or should the law protect listeners and viewers from this expression?

As the captivity problem indicates, exposure to harmful speech in networked public places will become increasingly difficult to regulate. The networking of public places will alter the form and character of public expression. It will, for example, permit speakers to use devices to virtually approach listeners and viewers. Network features will affect concepts such as imminence and risk, which have been critical to the application of First Amendment doctrines like fighting words, threats, and incitement to unlawful action. As public places become networked, we must consider what form of protection will be available to viewers and listeners when they encounter such things as mobile sexually explicit speech, virtual harassment, cyber-spamming, and other forms of harmful speech in public places.

The networking of public places will also substantially affect public protests and demonstrations. Networking features will facilitate assembly by providing platforms for social capital and the means for spontaneous

8. See *Cohen v. California*, 403 U.S. 15, 21-22 (1971) (holding that viewers must avert their eyes when confronted with offensive speech in courthouse corridors); *Rowan v. U.S. Post Office Dep’t*, 397 U.S. 728, 738 (1970) (“No one has a right to press even ‘good’ ideas on an unwilling recipient.”).

action. But they will also facilitate official and unofficial surveillance, as public and private cameras are increasingly used to record events in the public square. On balance, will the networking of public places render self-governing activities like protesting and petitioning too costly for most citizens?

The devices we carry, outfitted with Global Positioning System (GPS) technologies, will facilitate surveillance and tracking. The networked environment will compel us to constantly authenticate ourselves. Vast public areas will be under constant surveillance. In light of these eventualities, will the ability to shield speaker or associative identity be fundamentally compromised? Looking even further into the future, will biometric technologies, including those that can literally read faces, expose even private thoughts? Will digital environments compel us to speak in public against our will?

Finally, in a networked environment, should every citizen with the capacity to record and publish be deemed a member of the press? Should the truthful “reporting” of public events by “citizen-journalists” be shielded by the First Amendment from tort and other forms of civil liability, even when that reporting impinges on significant public privacy concerns?

Serious First Amendment concerns will be raised as the networking of public places proceeds. First Amendment doctrines and principles will be challenged by this transformation, just as they have been challenged by technological revolutions in the past. But the stakes of spatial networking are actually much higher than these doctrinal concerns indicate. Ultimately, we are facing a fundamental makeover of public places. Although they serve many purposes, public places are a collective democratic and expressive concern. They facilitate identity and equality claims. They allow for a wide variety of democratic participation. They lend transparency to both expressive claims and regulation of public expression. While we are considering First Amendment concerns, we ought also to ask how networked public places will affect core speech *values*, like self-government and civic interaction, in the traditional public marketplace of ideas. What will all of this networking do to public places?

The networking of public places will alter the nature, character, and democratic functions of public places and public expression. It will influence who speaks, where they may communicate, and what they will say. It will render speakers more knowable to authorities, but in many cases less knowable to one another. People will increasingly interact with devices in public, rather than with one another. Digitization will make some speech, and most speech regulation, less transparent to all of us. All of these changes threaten to render public places less capable of serving their traditional democratic functions.

The Article proceeds as follows: Part II will distinguish material public

places from networked ones, with specific attention to the speech implications inherent in the transformation of public places. It will describe the networking of public places—the technological, social, and environmental changes that are fundamentally transforming material public places. Part III will address the substantive First Amendment issues—public forum, public captivity, protection from harmful speech, protest, privacy, and press—raised by the networking of public places. Part IV will look beyond these primarily doctrinal considerations. Drawing upon urban geography and sociology literature, it will critically examine the civic character of networked public places in light of the First Amendment functions and values public places ideally ought to serve.

II. FROM MATERIAL TO NETWORKED PUBLIC PLACES

Much of First Amendment doctrine has developed with regard to a material model of public places. Public expression has taken place in a familiar cluster of places, from streets to malls to public squares to public parks. The first section of this Part will describe the general characteristics of public expression in material, non-networked public places. It will also touch upon the principal speech doctrines that have developed in this physical environment. The second section of this Part will describe the primary network technologies that will or are already reshaping public places and public expression. Three basic developments will be addressed. First, governments are currently providing, or partnering with private actors to provide, wireless Internet access in vast public areas. Second, governments have installed and are continuing to install surveillance equipment, including hundreds of thousands of CCTV monitors, in many public places. Third, individuals are carrying and wearing advanced communications technologies in public places. These devices will communicate with other devices and with the environment itself, which is also becoming embedded with computing devices.

A. *Speech in Material Public Places*

To understand the effect that the networking of public places will have on public expression, it is useful to begin with a brief discussion of the expressive characteristics that have traditionally defined material public places. In material places, the principles of geography, physicality, anonymity and equality have largely determined the contours of public expression.

The geography of material public places consists of bricks, mortar, and other tangible features. This geography provides the basic framework for public expression. In theory, the scope of public speech rights depends upon the geographic location the speaker inhabits. Thus, public streets, parks, and sidewalks are quintessential public forums in which speech

rights are at their apex.⁹ These places have “immemorially” been open for expressive purposes.¹⁰ Most other public places may or may not be open to expression, more or less at the government’s discretion.¹¹ Under the public forum and time, place, and manner doctrines, governments are entitled to maintain public and quasi-public places to effectively serve the governments’ primary purposes.¹² The primary purpose of most public and quasi-public places—the reason they were constructed—relates to concerns other than expression, such as traffic flow, travel, the provision of services, or recreation.¹³

The government’s relationship to geography or place is essentially that of a property manager or proprietor. Governments own the streets, parks, and other public places, in the sense that they have title to them. Governments have been responsible for providing whatever improvements or upgrades are necessary for the continued functioning of these places. Formally, governments have no interest in, indeed are forbidden from regulating, the content that is delivered by speakers to audiences on the streets, in the parks, or in other public places.¹⁴ Governments have never had any formal constitutional obligation to facilitate expression by building new places for it. Access to existing forums, however, has always been nominally available to all members of the public, regardless of a member’s means or status. There have never been public expression “fast lanes” on the streets for those with greater means.¹⁵

In their capacity as proprietors, governments have always observed and regulated public places. But they have done so mostly to ensure that a basic sense of order and decorum prevails there. Although there has always been some policing of public places, these activities have been subject to realities such as limited funding and manpower. Thus, at any given moment, most public places are not policed at all—in the sense that official eyes are not focused upon them.

The geography of public places has itself been used to police and to

9. See *Perry Educ. Ass’n v. Perry Local Educators’ Ass’n*, 460 U.S. 37, 45-46 (1983) (describing tiers of public fora).

10. See *Hague v. Comm. for Indus. Org.*, 307 U.S. 496, 515 (1939) (“Wherever the title of streets and parks may rest, they have immemorially been held in trust for the use of the public and, time out of mind, have been used for purposes of assembly, communicating thoughts between citizens, and discussing public questions.”).

11. See *Cornelius v. NAACP Legal Def. & Educ. Fund*, 473 U.S. 788, 802-03 (1985) (noting that governmental intent is a key indicator of forum status and expressive rights in public places).

12. See *Perry*, 460 U.S. at 45.

13. See, e.g., *Int’l Soc’y for Krishna Consciousness, Inc. v. Lee*, 460 U.S. 672, 682 (1992) (noting that airport terminal was constructed primarily for travel, not expressive activity).

14. See *Perry*, 460 U.S. at 45 (describing content neutrality requirement).

15. Of course, means are never entirely irrelevant. A speaker wishing to use certain public parks must, for example, have the means to pay the fee for a permit.

regulate public expression. The Supreme Court has held that the transmission of obscenity and other illegal content can be prohibited altogether to produce a certain “quality of life” and “tone of commerce” in public places.¹⁶ The time, place, and manner doctrine permits a government to zone or spatially restrict any speech it wishes, so long as the restriction is content-neutral, narrowly tailored, and leaves open ample alternative avenues of communication.¹⁷ In recent years officials have become experts at this zoning.¹⁸ Sexually explicit expression has been dispersed or concentrated spatially, purportedly to combat the “secondary effects” associated with it.¹⁹ Political displays of contention have increasingly been subjected to expressive zoning of various forms.²⁰ Zoning has become a very efficient means of sanitizing large public areas from expression that many may find quite offensive, harmful, or even just aesthetically distasteful.²¹

Geography and “spatiality” work in this fashion because public expression is itself physical, tangible, and grounded. It is intimately connected to and influenced by material places. This connection has rendered most public expression open and transparent. Confrontations, incitements to action, and demonstrations have generally been seen, experienced, and lived events. This fundamental fact has substantially shaped the contours of doctrines typically applied in public speech contexts. To define speech as a threat, for example, requires that the recipient have some reasonable fear of physical harm.²² A cross burning several feet from a back yard probably suffices to create the requisite fear.²³ Invitations to brawls (so-called “fighting words”), incitements to unlawful actions, and the idea of audience “hostility” are all based on

16. *Paris Adult Theatre I v. Slaton*, 413 U.S. 49, 57-58 (1973); *see also* *Miller v. California*, 413 U.S. 15 (1973) (defining “obscenity”).

17. *See Clark v. Cmty. for Creative Non-Violence*, 468 U.S. 288, 293 (1984) (noting that time, place, and manner regulations must be justified without regard to the content of speech, narrowly tailored to serve a significant government interest, and leave open ample alternative channels for communication).

18. *See Zick, Speech and Spatial Tactics*, *supra* note 7, at 589-606 (discussing spatial zoning tactics).

19. *See Young v. Am. Mini-Theatres, Inc.*, 427 U.S. 50 (1976) (upholding zoning of sexually explicit expression).

20. *See Zick, Speech and Spatial Tactics*, *supra* note 7, at 589-606 (describing various spatial restrictions).

21. *See Metromedia, Inc. v. City of San Diego*, 453 U.S. 490, 511-12 (1981) (plurality opinion) (indicating that a content-neutral ban on all outdoor advertising signs would be permissible).

22. *See Watts v. United States*, 394 U.S. 705, 708 (1969) (describing “true threats” doctrine).

23. *See Virginia v. Black*, 538 U.S. 343, 360 (2003) (stating that if requisite intent to intimidate the victim could be proven, a burning cross may constitute a “true threat”).

elements of proximity, immediacy, and visibility.²⁴ These content categories and scenarios can be effectively regulated under circumstances where the speech or speech acts can be witnessed, proven, and hence prosecuted. This was the underlying assumption when each of these categories was created.

Of course, the vast majority of public expression is neither illegal nor harmful to viewers or listeners. Thus, there is no reason to police it. As we go about our public lives, from sitting on a park bench reading a book to engaging in assemblies and peaceful protests with others, we expect that we are doing so anonymously.²⁵ In public places we are not, of course, *anonymous* in the sense that our identities are wholly private and cannot be discovered.²⁶ But when engaged in speech activities in public places, we do not expect to be constantly monitored. Beyond mere expectations, there is at least a minimal First Amendment right to remain anonymous in certain public settings. Thus, in *McIntyre v. Ohio Elections Commission*,²⁷ the Court invalidated an election law that prohibited the circulation of anonymous leaflets in connection with political campaigns.²⁸ The retention of anonymity in this circumstance is “a shield from the tyranny of the majority.”²⁹ It can be relied upon to “protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society.”³⁰

In a broader sense, whether or not we are engaged in core political pamphleteering we still expect that much of what we do in public will remain unremarked upon and unrecorded. We expect to blend into what Alan Westin has called the “situational landscape.”³¹ One can of course effectively undermine or even waive such an expectation. He may, for example, publicly burn a United States flag to garner attention for a cause

24. See *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969) (per curiam) (defining “incitement” category); *Feiner v. New York*, 340 U.S. 315, 320-21 (1951) (upholding disorderly conduct conviction where crowd had become hostile to speaker); *Chaplinsky v. New Hampshire*, 315 U.S. 568, 572 (1942) (defining fighting words as those which “tend to incite an immediate breach of the peace”).

25. For discussions of the principle of public anonymity, see Blitz, *supra* note 6, at 697-702; Slobogin, *supra* note 5, at 237-45.

26. See *United States v. Knotts*, 460 U.S. 276, 281 (1983) (“A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”); *United States v. Dionisio*, 410 U.S. 1, 14 (1973) (“No person can have a reasonable expectation that . . . his face will be a mystery to the world.”).

27. 514 U.S. 334 (1995).

28. *Id.* at 357.

29. *Id.* (citing JOHN STUART MILL, ON LIBERTY AND CONSIDERATIONS ON REPRESENTATIVE GOVERNMENT 1, 3-4 (R. B. McCallum ed., 1948)).

30. *Id.*

31. ALAN F. WESTIN, PRIVACY AND FREEDOM 31 (1967); see Blitz, *supra* note 6, at 683 (remarking on public anonymity and the “freedom to fade”).

or message.³² But barring this sort of activity, people in material public places quite reasonably have assumed that they can blend into a crowd.

This expectation has doubtlessly contributed to the shape of our public expressive culture. It has provided critical space for difference in public expression. That is not to say that speech in material public places is altogether free-wheeling, particularly in light of the proliferation of spatial controls and social norms that have limited it. But our public expressive culture has historically been one that has tolerated expression that is disruptive, boisterous, loud, and unconventional. In material public places, an expectation of public anonymity has provided speakers the freedom to engage in public displays that might otherwise have been substantially chilled.

Finally, in terms of general principles, material public places have historically been equalizing or leveling forces. Those lacking the means for more sophisticated expression have tended to use public places to convey messages that might otherwise have been silenced by market forces. Many “poorly financed causes of little people”³³ have relied upon places like streets, sidewalks, and areas surrounding facilities like airports, train stations, and public buildings to garner attention and convey messages. In this sense and others, public places and public expression have played a critical democratizing role in our society. Because this expression has been tangible and public, it has been quite difficult to ignore. At the least, public places have provided “little people”³⁴ an opportunity to interrupt the daily routine of public life and to force others to consider their claims.

The elements of geography, physicality, anonymity, and equality have substantially shaped the nature and tenor of our public expressive culture. As the next section will demonstrate, the networking of public places will affect each of these elements.

B. *The Networking of Public Places*

As mentioned in the Introduction, there are three primary features associated with the networking of public places. The first is the establishment, by governmental entities, of vast public Internet access networks. The second is the continued proliferation of surveillance devices

32. See *Texas v. Johnson*, 491 U.S. 397 (1989) (invalidating state law prohibiting the desecration of the flag).

33. *Martin v. City of Struthers*, 319 U.S. 141, 146 (1943). See generally Timothy Zick, *Space, Place, and Speech: The Expressive Topography*, 74 GEO. WASH. L. REV. 439 (2006) (discussing the importance of place to marginalized speakers and their expressive activity) [hereinafter Zick, *Space, Place, and Speech*].

34. See *Martin*, 319 U.S. at 146 (referring to the common members of society as the “little people”).

that continuously record public activity. And the third is the pervasive use of mobile personal computing devices in public places. This process of spatial networking will fundamentally change how information is conveyed, shared, and received in public places. It will alter the manner in which public places are policed and regulated. It will challenge and strain each of the fundamental precepts of material public places—geography, physicality, anonymity, and equality—discussed above.

1. Wireless Clouds—“Muni WiFi”

Urban “hot spots,” where anyone with the proper device can connect to the Internet, have been around for years. Some of the earliest wireless fidelity (WiFi) networks were patched together by Internet anarchists bent on creating a wireless commons.³⁵ Other early WiFi networks were the result of corporate-sponsored initiatives, meant to draw people to Starbucks and other quasi-public places and keep them there. For the first time, people were able to stay connected even while outside the home or office.

These were relatively small-scale experiments. But the early projects forecast an imminent intersection of so-called “cyberplaces” and material places on a much grander scale.³⁶ As the proprietors of vast public places, including many rural ones where Internet connectivity was spotty or simply non-existent, governments eventually became interested in providing WiFi to their citizenries.

WiFi is now draped over vast areas of public space. More than 200 cities, counties, and regions are currently providing or planning to provide some form of public wireless Internet access.³⁷ Increasing areas are now covered with wireless clouds or “meshes,” as the networks are often called. For example, Suffolk County on Long Island, New York, has installed a WiFi network that will reach some 1.5 million people and cover 900 square miles.³⁸ Philadelphia’s new WiFi network will cover most of the city’s approximately 135 square miles.³⁹ San Francisco is taking bids

35. See generally Kevin Werbach, *Supercommons: Toward a Unified Theory of Wireless Communication*, 82 TEX. L. REV. 863 (2004) (explaining concept of the wireless commons).

36. See generally Cohen, *supra* note 4 (critiquing the notion that “cyberspaces” constitute actual places).

37. MuniWireless, June 2006 Update of Wireless Cities and Counties in the U.S., <http://www.muniwireless.com/reports/docs/June-7-2006summary.pdf> (listing cities and regions that have developed Muni WiFi plans or already have operational networks).

38. Bruce Lambert, *Suffolk County Plans to Offer Free Wireless Internet Access*, N.Y. TIMES, Apr. 28, 2006, at B4.

39. Wireless Philadelphia Executive Committee, Briefing: A 21st Century Opportunity, <http://www.phila.gov/wireless/briefing.html> (last visited Oct. 1, 2006).

for an ambitious WiFi project.⁴⁰ New York City has already installed wireless hot spots in many of its vast park areas.⁴¹ New clouds are rising over cities and suburbs every day. Indeed, entire states aspire to become unified wireless communications networks.⁴²

Muni WiFi networks will provide public access to the Internet in parks, squares, public buildings, airport terminals, and literally wherever else citizens can carry their remote computing devices.⁴³ Some networks, like New York City's, will provide free connectivity, at least for now.⁴⁴ Other municipalities, concerned about expenses associated with developing and operating the wireless networks, plan to charge citizens for access.⁴⁵ Some, like San Francisco, have considered plans to offer "premium" connectivity for a fee, while relegating free users to a much slower connection speed.⁴⁶

There may be enormous educational and expressive benefits to Muni WiFi. In many rural communities, Muni WiFi will help close the digital divide.⁴⁷ It will enable activities like distance learning, coordinated policing, and other public services, and provide vast amounts of information to citizens. Despite these benefits, Muni WiFi has been a controversial undertaking. Until now, the provision of Internet access has primarily been a private venture. Bowing to pressure from the telecommunications industry, fifteen state legislatures have prohibited municipalities from offering public WiFi access.⁴⁸ At the time of writing, Congress is currently considering proposed legislation that would institute a nationwide ban, although the prospects for enactment appear slim.⁴⁹

40. Cf. Press Release, S.F. Dep't of Telecomm. & Info. Servs., San Francisco Concludes Evaluation of Proposals to Create Universal, Affordable Wireless Broadband Network (Apr. 5, 2006), available at http://www.sfgov.org/site/tech_connect_page.asp?id=38562.

41. Chan, *supra* note 1, at B5.

42. See, e.g., Noyes, *supra* note 1.

43. Although some municipalities have proposed offering access for free, perhaps supported by advertising revenue, the vast majority of the networks are subsidized.

44. See Sewell Chan, *Deadline Set for Wireless Internet in Parks*, N.Y. TIMES, May 16, 2006, at B1.

45. See, e.g., James Dao, *Philadelphia Hopes for a Wireless Lead*, N.Y. TIMES, Feb. 17, 2005, at A1.

46. See Laurie J. Flynn, *Some Worries as San Francisco Goes Wireless*, N.Y. TIMES, Apr. 10, 2006, at C3.

47. See Tim Gnatik, *Switchboard in the Sky*, N.Y. TIMES, May 3, 2006, at G1.

48. CNETNews.com, *Municipal Broadband Nationwide*, http://news.com.com/Municipal+broadband+and+wireless+projects+map/2009-1034_3-5690287.html (last visited Oct. 1, 2006) (detailing a map of the various Muni WiFi projects and state laws designed to limit them). The prohibiting legislation is described at MuniWireless, *Anti-Municipal Broadband Bills in the U.S.*, <http://muniwireless.com/municipal/579> (last visited Oct. 1, 2006).

49. Broadband Investment and Consumer Choice Act, S. 1504, 109th Cong. (2005). This is one of two dueling proposals in Congress. The other proposal would overturn the fifteen state bans, allowing municipalities and other state subdivisions to undertake WiFi projects. See Community Broadband Act of 2005, S. 1294, 109th Cong. (2005).

The principal arguments against Muni WiFi are based on efficiency concerns and the purported lack of need for the service. Telecom interests contend that there is no shortage of supply or market gap to fill.⁵⁰ Supporters of Muni WiFi suggest that the bottom line is the bottom line: Telecom companies want to provide public wireless access and reap the profits.⁵¹ On the merits, supporters argue that Muni WiFi is simply another utility—like electricity, roads, sewers, and water—that government should provide.⁵² Some, like San Francisco Mayor Gavin Newsom, have argued that Internet access is a “fundamental right” of the modern citizen.⁵³

Whatever the merits of the economic and rights arguments, efforts to stall or prevent the spread of Muni WiFi appear to be going nowhere. Public access to the Internet is already, or will shortly become, a reality in most large urban centers, an increasing number of suburbs, and many rural areas that have thus far been under-served in terms of Internet access.⁵⁴

Consideration of the full effects of Muni WiFi on public places and public expression must await a description of the remainder of the process by which material public places will become networked public places. But one can readily surmise some of the effects wireless clouds may have on the public expressive environment. In Parts III and IV, I will return to some of the themes sketched here.

Wireless clouds will alter the fundamental geography of material public places. To some extent they bring us closer to exploding the very concept of place itself. Cyberspace scholars often speak of the Web and other venues as separate virtual spaces.⁵⁵ But with public wireless access and other pervasive computing technologies, described below, where one happens to be will become far less important to one’s ability to communicate. To some extent terms like online and offline will cease to matter.

On-the-ground expression will be affected by wireless clouds floating above public places. The clouds will facilitate mobile communication and

50. See NEW MILLENNIUM RESEARCH COUNCIL, NOT IN THE PUBLIC INTEREST—THE MYTH OF MUNICIPAL WI-FI NETWORKS 2, <http://www.newmillenniumresearch.org/archive/wifireport2305.pdf> (February 2005) (noting that there is no shortage of broadband service in cities).

51. See, e.g., Carol Ellison, *Muni Wireless: The Battle Continues*, eWEEK.com, Jan. 25, 2005, <http://www.eweek.com/article2/0,1759,1754164,00.asp> (arguing that telecom companies’ interest in muni wi-fi is about market protection).

52. See Lawrence Lessig, *Why Your Broadband Sucks*, WIRED, Mar. 2005, available at <http://wired.com/wired/archive/13.03/view/html?pg=5> (arguing that municipalities should be allowed to compete in the wireless market and provide common good of wireless access as they have public roads).

53. Verne Kopytoff, *Fierce Wi-Fi Fight Expected In S.F.*, S.F. CHRON., Oct. 4, 2005, at C1.

54. See MuniWireless, *supra* note 37.

55. See Cohen, *supra* note 4 (discussing the idea that cyberspace is different from “real space”).

public information access. In networked public areas, private and public speech will mix and blend, as people bring the Web with them into public places. As a result, geography and place will become less reliable tools for restricting access and exposure to information that is harmful, offensive, or simply irritating. The Web will spill into public places.

The manner in which public speakers and audiences interact will also be affected by all of this cloud cover. Tangible and physical forms of expression will be replaced by virtual communications of various types. We are already increasingly distracted in public areas. Add to the cell phone and the MP3 player other mobile devices that connect to the Internet no matter where in public one happens to be, and people will be even more likely to engage devices rather than one another. The noise of the streets and parks will be replaced more and more by quiet concentration on personal screens. The very sights and sounds of public expression will change.

Wireless clouds will facilitate official and unofficial surveillance of public acts, including expression, association, and information-gathering. This will threaten public anonymity. Will the books or newspapers I am reading online as I sit on a park bench be recorded? Will my associations arouse suspicion? Will I even know?

The participants in public speech rituals and displays may also change. For those without personal computing devices, with no access or perhaps very slow access, the nature of public places will become that much more alienating and foreign. The digital divide that some experience at home will now go public, with new classes of haves and have-nots in public areas.⁵⁶ Public places may thus become less of an equalizing force.

2. Surveillance Square

Surveillance of public and quasi-public activities is not a new phenomenon. Private and quasi-public places have been under the camera's watchful eye since at least the late 1950s.⁵⁷ Banks were very early adopters of surveillance technologies. They used CCTV networks to monitor their vaults and their customers. Other commercial places, like malls and department stores, have also long placed customers and spaces under surveillance.⁵⁸

Two things, however, are very different in the modern era. The first is

56. See generally HIGH TECHNOLOGY AND LOW-INCOME COMMUNITIES: PROSPECTS FOR THE POSITIVE USE OF ADVANCED INFORMATION TECHNOLOGY (Donald A. Schön et al. eds., 1999) (discussing the scope of innovative technologies penetration into low-income urban areas).

57. Quentin Burrows, Note, *Scowl Because You're On Candid Camera: Privacy and Video Surveillance*, 31 VAL. U. L. REV. 1079, 1080 (1997).

58. *Id.*

the prevalence of public surveillance, in terms of both the numbers of cameras and the quantity of space they cover. The second is the technology itself, which enables surveillance that differs vastly in quality—that is, in the degree of its potential intrusiveness—from past generations.

Surveillance technology has become a mainstay of quintessentially public places like streets, city centers, and parks. The proliferation began in the streets, as officials sought new and efficient ways to police street crime.⁵⁹ Municipalities have long trained cameras on high-crime areas.⁶⁰ They later used these technologies for other purposes, for instance to cheaply and efficiently monitor traffic and issue citations for traffic violations.

Heightened security concerns, especially since the attacks of September 11, 2001, have led to the further proliferation of public surveillance.⁶¹ The United States has not yet reached the surveillance heights of Great Britain, “the champion of CCTV surveillance,” with between two and three million public cameras in operation.⁶² But at the mere start of developing a surveillance society, we already have hundreds of thousands of CCTV cameras watching over our public places. One scholar has suggested that video surveillance will likely “increase exponentially in the next decade.”⁶³

As one might expect, surveillance has recently become more prevalent in cities that may be at greatest risk from terrorist attacks. New York City has just begun to install and operate an extensive public surveillance system.⁶⁴ The city plans a first installment of 500 cameras, at a cost of \$9 million, with more to follow depending on the amount of funds received

59. See generally Raymond Surette, *Video Street Patrol: Media Technology and Street Crime*, 13 POLICE SCI. & ADMIN. 78 (1985) (discussing early uses of CCTV to police public crime).

60. *Id.* The primary official justification for these extensive official surveillance systems has been crime detection and prevention. There is a serious debate concerning whether this justification is empirically defensible. See Slobogin, *supra* note 5, at 224-30 (surveying evidence on crime prevention and deterrence).

61. This proliferation has also resulted in use of many privately maintained and operated video surveillance systems that are trained on public spaces. Many of the video feeds from these cameras can be linked to publicly operated surveillance systems. See Slobogin, *supra* note 5, at 222.

62. See *id.* British experience with CCTV has been extensively scrutinized. For a review of the literature, see Stephen Greenhalgh, *Literature Review of Privacy and Surveillance Affecting Social Behavior* (Aug. 2003) (unpublished manuscript on file with author).

63. Slobogin, *supra* note 5, at 219; see also Simon G. Davies, *Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity*, in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 150 (Philip E. Agre & Marc Rotenberg eds., 1997) (estimating 20-30% annual increase in public video surveillance).

64. See Tom Hays, *NYPD Deploys First of 500 Security Cameras*, ASSOCIATED PRESS, Apr. 16, 2006, available at <http://www.officer.com/article/printer.jsp?id=29927&siteSection=8>.

from the Federal Department of Homeland Security.⁶⁵ Ultimately the plan is to have several thousand wireless video cameras positioned atop lamp posts and on public buildings. New York City officials envision a “ring of steel” in parts of Lower Manhattan, one that resembles the plan recently implemented in London’s financial district.⁶⁶ The public surveillance plan is not limited to Manhattan. It calls for placing surveillance cameras throughout the five boroughs. Surveillance of underground public areas is also already widespread. New York City now has 1,000 cameras in its subway system, and expects to have over 2,000 in place by 2008.⁶⁷

The District of Columbia has also experienced a rapid rise in public surveillance. Large areas in and around the capital are under the jurisdiction of both local and federal authorities. The Metropolitan Police Department has a relatively modest public surveillance program. In 2002, for example, police used more than a dozen automated surveillance cameras to watch anti-war protests and a “March for Life” event.⁶⁸ The police department’s cameras are located throughout the National Mall and surrounding areas.⁶⁹ They target especially those places where marches and protests typically occur.

The National Park Service also operates surveillance cameras in and around various federal properties in the District, including the National Mall.⁷⁰ Unlike the D.C. surveillance system, which so far has been used primarily during large public events, the Park Service’s system is always operational.⁷¹ Thus, if you are near the White House or the Vietnam Memorial, for example, you are under surveillance.

Other large urban areas are increasingly implementing large-scale public surveillance projects. Chicago recently spent \$5 million adding 250 cameras to its current 2,000-camera system, one of the nation’s most extensive.⁷² Washington and Philadelphia have made similar

65. *Id.*

66. *Id.*

67. *Id.*

68. See *D.C. Police to Scan Crowds with Cameras*, MILWAUKEE J. SENTINEL, Dec. 21, 2002, at 05A.

69. See U.S. GENERAL ACCOUNTING OFFICE, VIDEO SURVEILLANCE: INFORMATION ON LAW ENFORCEMENT’S USE OF CLOSED-CIRCUIT TELEVISION TO MONITOR SELECTED FEDERAL PROPERTY IN WASHINGTON, D.C. 10-14 (June 2003) [hereinafter GAO REPORT] (describing D.C. Metropolitan Police Department’s use of CCTV).

70. See *id.* at 15-16.

71. *Id.* at 15. The District is considering authorizing daily use of surveillance cameras in certain areas. See Gary Emerling, *District Will Be Looking At You*, WASH. TIMES, Mar. 16, 2006, at A1.

72. Stephen Kinzer, *Chicago Moving to ‘Smart’ Surveillance Cameras*, N.Y. TIMES, Sept. 21, 2004, at A1.

investments.⁷³ However, the phenomenon is not limited to large cities. Cities like Tampa, Florida and Memphis, Tennessee, and even smaller municipalities have also recently invested in public surveillance programs.⁷⁴ As Department of Homeland Security grant money continues to flow to communities across the country, CCTV systems will likely become more and more prevalent, and potentially more intrusive, in public areas.

The latest generation of surveillance cameras has exceptional capabilities. Most have panning and tilting features. Some have zoom lenses “that can read the wording on a cigarette packet at 100 yards and bring nighttime images up to daylight level.”⁷⁵ Systems of the future will have features like motion detectors, facial recognition, biometric technology, and even X-ray or see-through capabilities.⁷⁶ The records these machines will create will also be different. Older technologies relied on conventional videotape for information storage. Newer CCTV technology will rely upon digitization.⁷⁷ This will make it easier to store information for much longer periods of time.

These advances are remarkable. As one organization recently put it, “[w]hat was once the grist of science fiction novels is quickly becoming the reality of modern law enforcement.”⁷⁸ With these surveillance technologies, it will be possible for authorities to identify, trace, and continually track a person the moment he enters the public square.⁷⁹ It will be possible to read what each citizen is reading, to see who he sees, to know where he has been and perhaps where he is going. It may at some point be possible to read his face by employing facial reading technologies. Much of this monitoring will be automated. The cameras will not operate in isolation. Along with public wireless networks and, as explained below, pervasive personal computing, surveillance technologies will be merely one aspect of a larger information network embedded in

73. See Hays, *supra* note 64 (noting recent CCTV expenditures by various municipalities).

74. See Slobogin, *supra* note 5, at 220 (“Newark, N.J., Tampa, Fl., Virginia Beach, Va., and Memphis, Tenn., all have cameras, ranging in number from six to seventy-two, that cover large areas of public real estate . . .”).

75. See *id.* at 222.

76. See *id.* at 223.

77. See *id.*

78. THE CONSTITUTION PROJECT, GUIDELINES FOR PUBLIC VIDEO SURVEILLANCE: A GUIDE TO PROTECTING COMMUNITIES AND PRESERVING CIVIL LIBERTIES 2 (2006), available at http://www.constitutionproject.org/pdf/video_surveillance_guidelines1.pdf.

79. In the UK, officials are preparing to initiate Celldar, a project that will permit surveillance of individuals based on the signals emitted from their cellphones. The system will allow officials to watch vehicles and individuals almost anywhere and any time, from up to hundreds of miles away. See Jason Burke & Peter Warren, *How Mobile Phones Let Spies See Our Every Move*, GUARDIAN UNLIMITED, Oct. 13, 2002, <http://www.guardian.co.uk/mobile/article/0,2763,811034,00.html>.

public places. The information collected will not merely disappear once the person leaves the public square. It will be retained and may even become part of a digital dossier.

The proliferation of public surveillance raises serious privacy concerns. In terms of public expression, these developments may change the geography of public space by marking off vast areas that will now be under public surveillance. Officials will no longer be limited to policing expression that they happen to witness on the scene and in real time. A less transparent but more efficient spatial regulatory regime will facilitate continuous policing of public areas.⁸⁰

Even if citizens do not know the details of surveillance, they will know that they are being watched. This may affect the books they read in public, the protests in which they are willing to participate, and the displays in which they are willing to take part in while in public places. The expectation of public anonymity will be undermined, if not entirely eliminated. The choice to reveal oneself and one's actions will no longer be the speaker's.

In terms of equality, certain "undesirable" populations, like the homeless or public agitators, may be displaced from certain areas as a result of constant surveillance. Those without the proper digital identification may be prevented from entering certain areas of the public square at all.

3. Pervasive Computing and Mobile Technologies

There is, finally, one additional feature that will complete the networking of public places. This element is perhaps the most critical to public communication and interaction. Networked places will not only have clouds hovering over them and cameras watching activity in them. The architecture of public places will be embedded with digital tags and networked information. Professors Jerry Kang and Dana Cuff call this already ongoing phenomenon "pervasive computing."⁸¹ Pervasive computing "is what happens when the Internet gets ubiquitous, embedded,

80. Despite the privacy and other implications of extensive CCTV use, at this point there is very little transparency in the adoption or use of the technology. Some municipalities have disclosed the location of their surveillance cameras. But other institutions, including the National Park Service, have not made this information public. See GAO REPORT, *supra* note 69, at 16. Few laws or regulations currently govern public CCTV use. Public participation in its adoption has been minimal. The Park Service, for example, has never sought public comment on its use of CCTV in areas of the National Mall. *Id.* at 4. Few municipalities have developed comprehensive controls for the use and operation of public surveillance, including protections for private data collected as a result of surveillance. See Slobogin, *supra* note 5, at 233-37.

81. Kang & Cuff, *supra* note 4, at 94.

and animated.”⁸² Professors Kang and Cuff describe the expected result of this embedding process: “Imagine not a robot, not an isolated and identifiable device, but a world saturated with networked intelligence.”⁸³

The digitally saturated world will give rise to new communicative forms, facilitate social networking, and produce a flow of environment-to-person communication not possible in inert material public places. The devices people wear or carry with them—personal computers, personal digital assistants, mobile telephones, and devices not yet conceived—will facilitate both person-to-person and person-to-place communication. Social interaction, including expressive activity, may change dramatically when, as Kang and Cuff put it, “a digital nervous system [is] grafted into the material world.”⁸⁴

In terms of expressive liberties, perhaps the greatest promise lies in the power the networked place will have to enhance social networking. As political scientists and sociologists have noted, contentious displays and social movements require social capital and coordinated action.⁸⁵ The Internet is already filling some of the gaps in otherwise frayed social networks.⁸⁶ Once in public places, protesters and demonstrators will be able to take advantage of pervasive networks to create smarter and more spontaneous assemblies. They will be able to use their personal devices to tactically assemble all at once, in places that are most effective.

This phenomenon has been referred to as “swarming.”⁸⁷ Even when it was limited to technologies of text messaging, swarming proved to be a powerful weapon of political dissent. During the 1999 World Trade Organization protests in Seattle, activists relied upon mobile phones and public networking to thwart some official efforts at repression.⁸⁸ With public Internet access now becoming widely available, swarming will likely migrate to the Web. Anyone with a connection will be able to participate, across media, seamlessly.

Smaller assemblies might also form as a result of pervasive and mobile communications devices. Digitized tags and GPS intelligence that we carry on our person will notify contacts in our vicinity of our precise location.⁸⁹ This could lead to spontaneous gatherings, as people quickly

82. *Id.*

83. *Id.* at 95.

84. *Id.* at 112.

85. See, e.g., BERT KLANDERMANS, *THE SOCIAL PSYCHOLOGY OF PROTEST* 15-16 (1997) (explaining processes of protest formation).

86. See ROBERT D. PUTNAM, *BOWLING ALONE: THE COLLAPSE AND REVIVAL OF AMERICAN COMMUNITY* 27 (2000) (noting the decline in social networks, community, and social capital).

87. See HOWARD RHEINGOLD, *SMART MOBS: THE NEXT SOCIAL REVOLUTION* ch. 7 (2002) (describing public swarming and its effect on political environments around the globe).

88. See *id.* at 160-62.

89. See Kang & Cuff, *supra* note 4, at 104 (“For instance, when you enter the shopping mall,

find one another in real time and real places. Through personal computing devices, we will also be able to leave digital trails of information to be found by those who come after us. The networked environment may become a dynamic digital bulletin board.

On a more retail or personal level, hand-held devices will enable strangers to learn bits of information about one another in public places.⁹⁰ Devices will “read” one another, allowing for a form of virtual personal reconnaissance.⁹¹ Bluetooth technologies will allow for virtual approaches and communication with those occupying the same public spaces and using similar devices.⁹² Right now, these opportunities are limited to those using similar devices and sharing the same network. But this phenomenon may someday extend beyond the similarly networked. One can already imagine a world in which each person has access to the same pervasive network.

Person-to-environment communication will be a frequent occurrence in networked public places. People will not merely traverse public places; they will interact with them.⁹³ The physical environment “will be able to respond directly to what it senses.”⁹⁴ As a speaker walks past a certain public place, she may receive an automated flow of information about conditions, directions, or dangers in that place.⁹⁵ She may automatically receive advertisements for products near that place, based on a geographic reading of her hand-held or worn device.⁹⁶ The flow of information will go in two directions. People will be able to communicate back to the environment and to interact with it.⁹⁷

Pervasive personal computing will also render each citizen a mobile recording unit. The cell phones they carry will enable not only

all friends in your social network who are nearby can be buzzed.”) (footnote omitted).

90. *See id.* at 110 (“PDA-sized gadgets that provide this sort of datasense about fellow conference attendees have already rolled out.”) (footnote omitted).

91. *See id.*

92. Bluetooth technologies facilitate the exchange of information between personal devices like cell phones and the connectivity of personal computing devices in close proximity to one another. *See* Wikipedia, Bluetooth, <http://en.wikipedia.org/wiki/Bluetooth> (last visited Oct. 2, 2006).

93. *See* John Markoff & Martin Fackler, *With a Cellphone As My Guide*, N.Y. TIMES, June 28, 2006, at C1 (describing phones that combine satellite technology with wireless web as “a missing link between cyberspace and the physical world”).

94. Kang & Cuff, *supra* note 4, at 94.

95. *Id.* at 110 (describing this information flow as “a sort of sixth sense, a *datasense*”). This will be made possible largely by the proliferation of embedded radio frequency identification (RFID) tags. *See id.* at 97-98 (describing RFID technology).

96. *Id.* at 110 (“As you pass by a commercial center, you receive a visual note on your dashboard that your favorite brand of shoes is on sale . . .”).

97. Kang and Cuff raise the possibility that public billboards may actually change content depending on who happens to be passing by a location. *Id.* at 112.

photography but also uploading of streaming video. Personal surveillance has already been a useful tool for protesters, who have used their own record of events to contradict what has been put forward by police as the official record of events on the street.⁹⁸ But there is a larger issue here. Pervasive computing devices will make on-the-scene reporting by citizens a much more common event. There are already projects underway creating spaces on the Web that will act as public clearinghouses for photos, videos, and reporting sent in by citizens all over the world.⁹⁹ When we are in public, we will be watched not only by officials, but by an army of citizen-journalists too.

The digital nervous system and personal computing appendages attached to it will alter fundamental features of material public places. The geography will no longer be something we merely stand or walk upon. We will interact through and with it. As noted above, the mobility of expression will confound efforts to spatially regulate it. As public speech becomes more and more digital and virtual, it will lose its traditional tangible and physical character. Listeners and viewers will communicate via an additional sense, what Kang and Cuff call a “datasense.”¹⁰⁰ Virtual expression and “datasensing” will be more difficult to police, in part because these communications will not be physical and visible.

In addition, the mobile technologies we carry or wear will allow us constantly to be identified and authenticated as we pass through physical places.¹⁰¹ Public anonymity will be further diluted. The basic choice *whether* to speak will no longer be completely our own. Disclosure will be automated; in some sense expression will be a product of our consent to carrying or wearing the latest devices as we travel around in public. As noted, some people carrying those devices will be able to “report” on the acts of others, adding another layer of public surveillance. Finally, in terms of the traditional equality of material places, only the digitally privileged will be able to participate fully in networked public places. The digital nervous system will be possessed only by those who possess the latest technologies. The new have-nots will be missing more than a critical hardware and computer connection: They will lack an increasingly critical sense—a datasense.

98. See *infra* note 314 and accompanying text.

99. See Mark Glaser, *Stanford Fellow Imagines Every Cell Phone as Citizen Media Outlet*, MEDIASHIFT, July 18, 2006, http://www.pbs.org/mediashift/2006/07/digging_deeperstanford_fellow.html. A mockup of such a site is available at www.inthefieldonline.net.

100. Kang & Cuff, *supra* note 4, at 110.

101. *Id.* at 106; see also Kevin D. Werbach, *Sensors and Sensibilities* 28 CARDOZO L. REV. (forthcoming 2007) (noting that universal connectivity will facilitate the tracking of individuals).

III. FREEDOM OF EXPRESSION IN NETWORKED PUBLIC PLACES

This Part will translate the geography, physicality, anonymity, and equality concerns raised by the networking of public places into explicit First Amendment concerns. Most of the commentary, in legal and social science communities, has centered upon the effect surveillance technologies will have on privacy rights.¹⁰² Cameras are only a single feature of a much larger and more sophisticated network. The “digital nervous system” is, or at some point will be, an *integrated* system. Surveillance cameras will be linked to public Web access. Mobile data tags will be linked to surveillance technologies. Personal computing devices will link to the environment, to other devices, to surveillance networks, and to various information clearinghouses on the Web. The progression to networked public places will affect a variety of First Amendment principles and doctrines.

A. *Property: The Legal Status of Wireless Clouds*

Large-scale municipal wireless projects have been greeted as either the unremarkable provision of an important public utility or an unnecessary and unwise interference with traditional private provision of Web access. Mostly ignored so far have been the serious free speech concerns that arise as governments step in to provide direct access to a critical communicative medium like the Internet.

In terms of the provision of communicative infrastructure, Muni WiFi clouds are unprecedented. How should we conceptualize the wireless clouds hanging over public areas? We might view the provision of public Internet access as analogous to the provision of water, electricity, or other public utilities. In one sense the analogy has some merit. As they have in other public goods contexts, governments are stepping in and providing, or partnering with private entities to provide, a critical public infrastructure. This is what happened with electricity and sewers. Internet connectivity, one might say, is fast becoming as critical to the modern citizen as these other services. Governments thus naturally ought to provide the service of public connectivity.

Ultimately, however, this analogy to public utilities is fundamentally flawed. For one thing, there is already a flourishing private market for the provision of Internet access. At least in many urban and suburban areas, a network of hot spots has been developing for some time. With private providers seemingly in no short supply, one might wonder if there is really

102. Professors Kang and Cuff do adopt a somewhat broader perspective. As discussed in Part IV, *infra*, they examine the implications of pervasive computing for the health of the public sphere generally. See Kang & Cuff, *supra* note 4, at 115-21; see also Blitz, *supra* note 6, at 697-702 (discussing First Amendment anonymity concerns related to public surveillance).

some market failure to correct. As a matter solely of economics, then, there may be sound reasons for governments to stay out of the Internet connectivity market.

But the analogy to other public services suffers from a much deeper flaw than market economics indicate. Simply put, electricity and sewage are nothing like the information that will flow as a result of wireless clouds and meshes. Governmental provision of electricity, for example, raises no serious constitutional concerns. Assuming the service has not been entirely privatized, thus removing constitutional concerns, governments must merely refrain from inequitable provision of services and satisfy basic due process requirements.¹⁰³ But Muni Wi-Fi is no ordinary public utility in this regard.

For the first time, governments (and in some cases their private partners as state actors) will provide and control the backbone of a communications network over which vast amounts of public communications will flow. This invokes an altogether different analogy. Putting wireless clouds in the sky is like building a public road *solely for communicative purposes*. This is much more akin to providing an expressive forum than a mere public utility. When governments provide access to information through such forums, First Amendment issues of access and content control inevitably arise. Government provision of wireless clouds will likely raise similar issues. Suppose, for example, a municipality is not willing to provide unfettered connectivity. As noted, the Web defies the sort of spatial control that material places often facilitate. Owing to its architecture, access to the Web is not partial. How long will it be before concerned citizens or groups object to public provision of access to pornography, or hateful expression, or morally offensive materials? How long before suspected terrorists are tracked through the public network? Or suppose a citizen claims a right of access to the portal site to convey a message. Does she have a right to post information there?

Although the scope of Muni WiFi projects is unprecedented, this is not the first time that government has provided Internet access in a public place. Nor is it the first time government has confronted issues relating to Internet access control. By 2000, 95% of public libraries were offering Internet access, most through a federal funding program.¹⁰⁴ When public libraries installed their Internet connections, the entire Web flowed into the library space, much as Muni WiFi will introduce the Web to larger public areas. Reports of adults and children accessing sexually explicit materials in public libraries, and of patrons exposing others to this

103. See, e.g., *Jackson v. Metro. Edison Co.*, 419 U.S. 345 (1974) (holding that due process and equal protection claims could not be brought against a private utility).

104. See *United States v. Am. Library Ass'n*, 539 U.S. 194, 199 (2003).

material, quickly began to surface.¹⁰⁵ When this situation came to Congress's attention, it enacted the Children's Internet Protection Act,¹⁰⁶ which requires that libraries take steps to prevent access to obscenity, child pornography, and materials deemed harmful to minors or face the loss of certain federal funds.¹⁰⁷

The libraries sued, arguing that filtering patron access was an infringement on patrons' First Amendment rights and undermined their own mission to provide access to the widest possible range of information.¹⁰⁸ The Supreme Court dismissed these arguments.¹⁰⁹ It noted that public libraries had always exercised discretion in selecting collection materials and that sexually explicit materials have historically not been found on their shelves.¹¹⁰ Moreover, the Court noted that neither a public library's collection nor the Web itself is a "forum" for expressive purposes.¹¹¹ The Internet, the Court noted, was of far too recent vintage to be considered a quintessential public forum like a street or park.¹¹² Moreover, according to the Court, libraries do not provide Internet access to encourage the dissemination of a variety of viewpoints; rather, they provide it for the same reasons they provide access to other materials—for education, research, and recreation.¹¹³ Thus, no speaker could claim a right to use a public library's Internet service to reach a public audience.

What does the library experience suggest about the legal and constitutional status of governmentally installed wireless clouds? As the Court noted in the library context, the Web itself cannot be deemed a "traditional" public forum because this resource is simply too *new* to have been "immemorially . . . held in trust for the use of the public."¹¹⁴ Governmental provision of Internet access is yet another circumstance that highlights the inflexibility of the Court's rules for categorizing public

105. See *id.* at 200 (describing evidence of patron access). A much fuller account of public library experiences with Internet access can be found in the opinion of the trial court three-judge panel. See *United States v. Am. Library Ass'n*, 201 F. Supp. 2d 401, 422-27 (E.D. Pa. 2002), *rev'd*, 539 U.S. 194 (2003).

106. Pub. L. No. 106-554 tit. XVII, 114 Stat. 2763A-335 (2000).

107. 20 U.S.C.A. § 9134(f) (West 2006); 47 U.S.C.A. § 254(h)(6) (West 2006).

108. *Am. Library Ass'n*, 539 U.S. at 210.

109. *Id.* at 211. The author wishes to disclose that he worked on this case on the government's behalf in the lower courts.

110. See *id.* at 205 ("Public library staffs necessarily consider content in making collection decisions and enjoy broad discretion in making them.").

111. *Id.* at 206.

112. *Id.* at 205-06.

113. *Id.* at 206.

114. See *Int'l Soc'y for Krishna Consciousness, Inc. v. Lee*, 505 U.S. 672, 679 (1992) (limiting category of "traditional" public forums to include only streets, sidewalks, and public parks).

places.¹¹⁵ Through Muni WiFi programs, the Internet is becoming a resource held in trust for public communicative activity. Under current doctrine, however, the wireless clouds do not create a traditional expressive forum.

It is more likely that by providing a link to the Internet, municipalities are displaying the requisite intent to establish a “designated” public forum for the exchange of a diversity of ideas and information.¹¹⁶ Unlike public libraries, municipalities have not historically exercised editorial discretion in terms of the content conveyed in public places. Indeed, they are generally forbidden under the First Amendment from taking the content of expression into account. And unlike libraries, municipalities *are* providing the connection to encourage the dissemination of a variety of viewpoints. Thus, any municipal filtering of public Internet access would have to meet the highest standard of judicial scrutiny.¹¹⁷

Even if a municipality could convincingly argue that it had a compelling interest to filter (for example, to protect children from public exposure to certain materials deemed harmful to minors), it is doubtful that any sufficiently tailored means for serving that interest could be fashioned. Filters are certainly far more technologically advanced today than they were a decade or more ago. But no filter can currently screen solely illegal content from the Web, leaving the remainder undisturbed.¹¹⁸ Under the statutes regulating Internet access in public libraries, patrons can simply request that a librarian unblock a website if they are denied access.¹¹⁹ However workable this sort of system might be in the limited public space of the library, it cannot be used in vast public areas. Who would decide whether to unblock a site? On what basis? Pursuant to what procedures?

Nor will any citizen likely prevail in asserting an access claim to the public Web portal site. Assuming advertising or other speech does not appear there, the portal site likely would be deemed a non-public forum. Municipalities could thus prohibit private expression there. Use of the network will be protected; use of the portal will not be.

Having created a forum with its wireless clouds, a municipality will

115. See Zick, *Space, Place, and Speech*, *supra* note 33, at 456-59 (describing primary criticisms of public forum doctrine).

116. See *Cornelius v. NAACP Legal Def. & Educ. Fund, Inc.*, 473 U.S. 788, 802-03 (1985) (noting that government must make an affirmative choice to open a “designated” public forum).

117. It is unlikely that municipalities will grant speakers right of access to any home or registration page they use as a portal. Unless governments open that space to diverse expression, the homepage would likely constitute a non-public forum, a resource generally under governmental control.

118. See *United States v. Am. Library Ass’n*, 201 F. Supp. 2d 401, 449 (2002), *rev’d*, 539 U.S. 194 (2003) (noting that filters routinely block innocuous materials).

119. See Children’s Internet Protection Act, 20 U.S.C. § 9134(f)(3) (2000) (disabling of filter permitted for adults and minors).

have no choice but to provide the entirety of the Web in public places. The Web will spill into the public square, just as it initially flowed into the public libraries. Public exposure to expression that might once have been the province of home-bound devices has already begun to raise privacy and public captivity concerns. We shall turn to these next.

B. Public "Captivity"

The ubiquity of the Web, combined with pervasive and mobile computing devices, will alter accepted notions of private and public expression. We may become captives to public expression we do not wish to see or hear. Technologies like mobile phones and other personal devices will thrust speech on unwilling audiences in public places, on the streets, on buses and subways, and in parks.

Some of this expression will be sexually explicit. Cell phone providers are already providing pornographic content in other countries; the U.S. market is not far behind.¹²⁰ This will make it possible to view sexually explicit content virtually anywhere, anytime. Several complaints have already been raised by drivers who were subjected to a nearby car's playing of a pornographic DVD, which is clearly visible, especially during evening hours.¹²¹ As well, new forms of targeted advertising or spamming that rely upon the GPS features in personal devices will bombard an already advertising-saturated public.¹²² Will the First Amendment permit any reprieve from these potential nuisances?

The First Amendment provides some limited protection for the captive listener or viewer who cannot reasonably avoid unwanted expression. Just as there are rights to see or hear expression, there are corollary rights not to see or hear.¹²³ The right to be let alone is most vigorously enforced when the listener or viewer is in the home, because of the strength of the privacy interest in that place and the practical difficulties of avoidance.¹²⁴

120. See Gary Strauss, *Cellphone Technology Rings in Pornography in USA*, USA TODAY, Dec. 13, 2005, at 1D, available at http://www.usatoday.com/tech/products/services/2005-12-12-pornography-cellphones_x.htm.

121. See *Playing at an SUV Near You: Porn*, CBS NEWS, Mar. 11, 2004, <http://www.cbsnews.com/stories/2004/03/11/national/main605394.shtml> (reporting incidents of pornography displayed in vehicles).

122. See generally Adam Mossoff, *Spam—Oy, What a Nuisance!*, 19 BERKELEY TECH. L.J. 625 (2004) (discussing the problem of unsolicited email correspondence, or "spam").

123. See *Lehman v. City of Shaker Heights*, 418 U.S. 298 (1974) (recognizing limited right not to receive information); see also Franklyn S. Haiman, *Speech v. Privacy: Is There a Right Not to Be Spoken To?*, 67 NW. U. L. REV. 153 (1972) (discussing doctrine of captivity).

124. See *Frisby v. Schultz*, 487 U.S. 474, 484-85 (1988) (discussing private captivity cases). Even in the home, a viewer or listener must often resort to self-help, such as depositing objectionable mail in the waste basket. *Consol. Edison Co. of N.Y., Inc. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 530, 542 (1980) (footnote omitted).

New technologies always pose distinct problems in terms of their ability to thrust content into places like the home. In *FCC v. Pacifica Foundation*,¹²⁵ for example, the Supreme Court upheld federal regulations prohibiting the broadcast of “indecent” expression over the airwaves during certain hours of the day when children and unwilling adults might be listening.¹²⁶ The Court reasoned that radio broadcasts of indecent expression were akin to an “assault” from which homeowners were entitled to some protection.¹²⁷ Similar reasoning was recently invoked by courts to uphold the federal “do-not-call registry,” which prevents most telephone solicitors from disturbing people while at home.¹²⁸

In public places, however, self-help is the primary means of protection from unwanted expression. The listener or viewer is generally expected to avert her eyes from public expression she does not care to see or hear. In *Cohen v. California*,¹²⁹ the Court held that viewers in public courthouse corridors could protect themselves by averting their eyes from Cohen’s offensive jacket, which was emblazoned with the words “Fuck the Draft.”¹³⁰ In *Erznoznik v. City of Jacksonville*,¹³¹ the Court invalidated an ordinance that would have banned all nudity in outdoor movie theatres.¹³² The audience, even while driving on the public highways and thus potentially (and quite dangerously) distracted by the display, was required to turn a blind eye to what appeared on the screen.¹³³

The networking of public places will challenge fundamental notions of public and private. The mobility of private forms of expression will render those private forms increasingly a matter of public concern. When public places are networked, it may become increasingly difficult to maintain a basic level of public repose. The “assaults” may come from many directions at once. Private offensive expression will move closer and closer to unwilling or undecided audiences. The nudity on the public movie screen will appear on the screen in the car sitting in traffic in front

125. 438 U.S. 726 (1978).

126. *Id.* at 738.

127. *Id.* at 748-49.

128. *See* *FTC v. Mainstream Mktg. Servs., Inc.*, 345 F.3d 850 (10th Cir. 2003) (per curiam) (upholding federal “do-not-call” registry).

129. 403 U.S. 15 (1971).

130. *Id.* at 21.

131. 422 U.S. 205 (1975).

132. *Id.* at 213.

133. In one instance the Supreme Court did embrace something like the right to be let alone in a quintessential public forum. In *Hill v. Colorado*, the Court upheld an 8-foot bubble between abortion clinic sidewalk counselors and clinic patrons on public sidewalks. 530 U.S. 703, 726-27 (2000). In that context, the Court said, a woman was entitled to some protection for her psychological repose. *See id.* at 717-18. The Court, however, has shown no inclination to extend the right to be let alone to other public areas.

of you. The pornographic magazine will be digitized and transported onto the subway or bus, or into a public park, airport terminal, or other public place.¹³⁴

One would expect (or at least hope) that social norms and decorum would prevent the most intrusive encroachments on others' public tranquility and repose. But if some drivers are willing to view sexually explicit material in the car on a public road or in a parking lot, what will stop them from doing so in other public places?¹³⁵ Carrying explicit magazines into public places like buses and parks is quite different, in social terms, from transporting it by way of personal computing devices. The latter have already achieved a substantial degree of public acceptance. They are fast becoming perceived human necessities. They are part of the public environment.

Right now, the doctrine or principle of captivity offers very little protection for the unwilling recipient of public expression. But cases like *Cohen* and *Erznoznik* were decided before mobile content devices proliferated in public places. These decisions were products of a model of public expression based upon material, not networked, places. That model generally facilitated a spatial segregation of offensive expression no longer possible in networked public places. The question is whether the networking of public places counsels a change in principle when it comes to public captivity.

Although it has been reluctant to grant the unwilling audience broad rights to be let alone in public, the Court has indicated that the matter requires "delicate balancing."¹³⁶ On one hand, new technologies will make it easier to thrust expression into the visual and auditory fields of unwilling audiences, including children, thus affecting the tranquility and livability of public places. On the other hand, we are becoming all too proficient at filtering out the background and foreground noises of everyday life. We already use personal computing devices to defend ourselves from outside interferences and to build a wall of separation between ourselves and others.

Cases like buses and subway cars remain most problematic, given the difficulties of escaping unwanted speech and the reliance upon these

134. For those who doubt the possibility, the author offers one personal anecdote. Recently, while sitting in a café, I witnessed a patron viewing a pornographic website on his laptop in full view of other patrons, including several children. The parents quickly removed the children. The adults, including the author, pretended not to notice.

135. The limits of reliance upon social norms are apparent on the subways. In New York City, there have been several recent arrests for sexually menacing behavior like flashing. See Anemona Hartocollis, *Women Have Seen It All on Subway, Unwillingly*, N.Y. TIMES, June 24, 2006, at A1 (reporting incidents of flashing and groping on city subways).

136. *Erznoznik*, 422 U.S. at 208.

modes of transportation by many people. But one might surmise that few today would be as distressed as Justice Douglas was in *Public Utilities Commission v. Pollak*¹³⁷ at the prospect of radio transmissions being piped onto public buses.¹³⁸ Douglas, in dissent, strongly objected to the invasion of public privacy and repose brought about by these transmissions, in no small part because the government had something to do with their content.¹³⁹ Today's rider may not even hear such transmissions, so ensconced is she in her own technological bubble. One might also suspect that our sensibilities, including our expectations with regard to public repose, have changed dramatically since the 1950s. Justice Douglas's outrage was in some sense a product of his times. Modern citizens' tolerance for the thrusting of expression is likely much higher, by sheer necessity, than that of generations past.

We have not yet reached a point where freedom of expression must give way to a public right of repose or tranquility. But this may change depending on our experiences in networked public places. The Supreme Court has, at least in one context, supported the right of listeners to be let alone in public places.¹⁴⁰ There are already laws under consideration that would criminalize the display of sexually explicit images in cars.¹⁴¹ Whether the push for new laws to protect the unwilling listener or viewer will be more widespread is impossible to know at this point. From a normative perspective, however, it does seem rather incongruent for people to simultaneously disappear into personalized bubbles and at the same time demand legal protection from expression they do not wish to see or hear.

Sex will not be the only speech thrust upon citizens in networked public places. The same basic calculus applies to aggressive advertising or what might be referred to as "public spamming." Pervasive computing will open up new possibilities for consumer targeting, including advertisements based upon the recipient's present geographical location. The environment itself will communicate offers to passersby. Many of these communications will be unwanted, in the sense that the recipient will not directly solicit them.

Concerns about aggressive or manipulative advertising arise with each new generation of technologies. In the 1970s, for example, concerns were raised about Madison Avenue tactics that might be subsumed under the

137. 343 U.S. 451 (1952).

138. See *id.* at 468 (Douglas, J., dissenting).

139. *Id.* at 469 (likening program to a form of mind control).

140. See *Hill v. Colorado*, 530 U.S. 703, 718 (2000) (noting strong public interest in protecting repose of abortion clinic patrons).

141. See, e.g., TENN. CODE ANN. § 55-8-187 (West 2005); VA. CODE ANN. § 46.2-1077.01 (West 2006).

heading “subliminal advertising.”¹⁴² The email spam that stuffs our daily inboxes is only the latest example of commercial exploitation of new technologies. Public spamming would merely be the natural next generation of this phenomenon.

The differences, however, between previous instances of aggressive advertising and what may become large-scale public spamming rest both on notions of place and technological self-help. Private spamming and harassing advertising are particularly troublesome because they invade the home. As noted, however, we enter the public sphere with a very limited expectation of privacy. In public places, we are already bombarded with commercial advertisements. As distasteful as some of these pleas are, as long as they are not false and misleading they are protected expression.¹⁴³ Although their time, place, and manner of delivery can be regulated if sufficiently important reasons warrant, they cannot be prohibited.¹⁴⁴ Just as we daily exercise selective attention and memory to deal with those ads, so too will we have to learn to ignore digitally delivered ads while we are in public places.

This assumes, of course, that the advertisements ever reach us. If we do not wish to receive them, we will presumably find a way to program our personal devices to filter them out.¹⁴⁵ Or we will walk away from the place that is facilitating the transmission. Or, if one can imagine such a thing, we will simply turn the device off. Increasingly the power of avoidance will lie precisely where the power of delivery does—in the technology we hold in our hands or wear on our bodies.

The networking of public places will bring vast amounts of previously private expressive content into public view. Barring some rather serious doctrinal reconsideration, which at this point seems unlikely and probably in any event unnecessary, we will likely have to tolerate more offensive and aggressive forms of public expression in networked public places. Self-help, in terms of both social practices and technological solutions, will be the primary recourse when unwanted expression intrudes on the privacy and repose of unwilling audiences.

142. See Nicole Grattan Pearson, Note, *Subliminal Speech: Is It Worthy of First Amendment Protection?*, 4 S. CAL. INTERDISC. L.J. 775, 778 (1995); see also Olivia Goodkin & Maureen Ann Phillips, *The Subconscious Taken Captive: A Social, Ethical, and Legal Analysis of Subliminal Communication Technology*, 54 S. CAL. L. REV. 1077 (1980-81) (discussing the use of subliminal communication technology up until 1980).

143. See *Va. Bd. of Pharmacy v. Va. Citizens Consumer Council*, 425 U.S. 748 (1976) (holding that commercial speech is protected by First Amendment).

144. *Id.* at 771.

145. See CASS R. SUNSTEIN, *WHY SOCIETIES NEED DISSENT* 107 (2003) [hereinafter SUNSTEIN, *DISSENT*] (discussing private programming of communications technologies to cater to personal interests).

C. *Protection: Dangerous, Offensive, and Harmful Speech Activity*

Public captivity raises an even larger concern with respect to the presence of harmful or dangerous speech in networked public places. As noted in Part II, in material public places expression—and its regulation—tends to be tangible and physical. Assuming some minimal advance notice, a listener or viewer can generally avoid speech by avoiding the speaker, or the place. The tangibility and visibility of expression in material places also facilitates its official regulation. Doctrines like true threats, fighting words, harassment, and incitement are based on a material model of public places and public expression. Expression in networked public places is already beginning to lose its tangible and physical characteristics. What protection will there be for audiences, and the public at large, from harmful expression in networked public places that is digitally conveyed?

New technologies invariably give rise to new forms of annoying and harassing expressive behavior. There may in fact turn out to be a number of annoying and embarrassing applications of new technologies in networked public places. For example, there have been public voyeurism issues related to recent uses of personal cameras in public places.¹⁴⁶ Today it is relatively easy to take a photograph of a person in public, perhaps doctor the image in any number of ways, and post it immediately on a website for all to see. Soon a single device like a cell phone will serve all of these purposes at once.

More seriously, in networked public places it may soon be possible to approach a recipient *virtually*, perhaps anonymously. Devices will “introduce” themselves to other nearby devices.¹⁴⁷ This type of communication, along with public spamming, may introduce new forms of harmful speech. We may encounter an updated virtual version of the sidewalk harassment that occurs with disturbing frequency in material public places.¹⁴⁸ The public audience may also be vulnerable to an even more pernicious form of harassment that we might call “public cyber-stalking.”¹⁴⁹ This is not, admittedly, a current problem, in part owing to

146. See H. Koskela, *Video Surveillance, Gender and the Safety of Public Urban Space: “Peeping Tom” Goes High Tech?*, 23 URBAN GEOGRAPHY 257, 257-78 (2002).

147. For example, recently launched Bluetooth technology called “Proximating” notifies a user when a potentially compatible mate is nearby. See Proximating, *The First Ever Bluetooth Proximity Dating Software*, http://www.proximating.com/index.php?code_pays=US (last visited Sept. 24, 2006) (“Imagine, you are crossing the street when the girl/boy of your dreams passes before you, your phone buzzes and their face appears on your phone’s screen . . .”).

148. For a recent analysis of sidewalk harassment, see LAURA BETH NIELSEN, *LICENSE TO HARASS: LAW, HIERARCHY, AND OFFENSIVE PUBLIC SPEECH* (2004).

149. Cyber-stalking is the use of communications devices to stalk another. See U.S. DEP’T OF

Americans' relative slowness in adopting new peer-to-peer technologies.¹⁵⁰ But consider that a mere decade ago, few had even heard of cyber-stalking. As a result of some pervasive online misconduct, today many states have laws that purport to protect unwilling recipients from harassing, annoying, and even embarrassing online communications.¹⁵¹ What, if any, protection can or should these or other laws provide from new forms of harmful expression produced by and in networked public places?¹⁵²

There are obvious constitutional problems with protecting any of us from merely annoying or embarrassing expression, as some cyber-stalking laws purport to do.¹⁵³ The networked public environment will often be an annoying place to be. Opportunities for public embarrassment will rise as cameras capture public events. But assuming the communication is delivered through an online medium, with the requisite intent and the effect of causing a reasonable fear of harm, existing statutes would appear to protect the victim of public cyber-stalking. There is no reason to limit application of these statutes to instances in which the victim is in the home or workplace when she receives the communications. The harm is the psychological damage the fear engenders, and that fear may be even greater in an open public place where the victim may be more physically exposed and vulnerable. So long as the victim knows or reasonably fears she is being stalked, the statutes should apply.¹⁵⁴

The concerns with public cyber-stalking are ultimately not legal, but pragmatic ones. Even with ubiquitous CCTV and other forms of surveillance, the likelihood of real-time official intervention is quite slim. Technological advances are also making proof of these offenses

JUSTICE, 1999 REPORT ON CYBERSTALKING: A NEW CHALLENGE FOR LAW ENFORCEMENT AND INDUSTRY, available at <http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm>.

150. Americans have been less apt to adopt peer-to-peer technologies like Bluetooth systems than, say, Japanese citizens. But if the cost of these technologies decreases, as expected, we may see substantial changes in communicative habits in public places. See RHEINGOLD, *supra* note 87, at 22-24 (discussing economic and cultural influences).

151. See Eugene Volokh, *Freedom of Speech in Cyberspace from the Listener's Perspective: Private Speech Restrictions, Libel, State Action, Harassment, and Sex*, 1996 U. CHI. LEGAL F. 377 (describing and analyzing cyber-stalking laws).

152. Connectivity has created difficulties in the workplace as well. See David T. Bower, Note, *Make It Stop or I'll Sue!: The Feasibility of a Hostile Work Environment Claim Created by Sexually Explicit Spam*, 90 IOWA L. REV. 1577 (2005) (noting the rising problem of sexually explicit workplace spam).

153. See Volokh, *supra* note 151, at 425-35 (discussing vagueness and overbreadth problems with many cyber-stalking laws); see also Joshua Azriel, *First Amendment Implications for E-mail Threats: Are There Any Free Speech Protections?*, 23 J. MARSHALL J. COMPUTER & INFO. L. 845 (2005) (discussing First Amendment implications of regulating email threats).

154. See *Frazier v. Delco Elecs. Corp.*, 263 F.3d 663, 668 (7th Cir. 2001) ("The stalking victim who doesn't know that she is being stalked is not in fear of being injured.").

increasingly difficult. A sustained stream of communication to one's home or work computer may produce a record of evidence sufficient to identify, arrest, and prosecute a wrongdoer. But a quickly delivered and perhaps encrypted strike in a public place, or even a series of them, will be difficult to trace, track, and police. Now add one more twist to our public cyber-stalking scenario. It is currently possible to send self-destructing virtual communications—messages that explode and essentially disappear shortly after they are received.¹⁵⁵ Under these circumstances, proof and prosecution under threat or other safety laws will be most difficult if not altogether impossible.

It would seem that, as in material places, the merely annoying and embarrassing will either have to be tolerated or policed by social norms and self-help mechanisms. The recipient or target of harassing expression in networked public places will have at her disposal substantial means of self-help. She might of course leave the park, mall, or other place. But as occurs in some traditional harassment and stalking situations, she may be followed. Or she may reset her device's receipt protocols to block any further messages from the particular speaker. This may be the best defense against at least some forms of public cyber-harassment. We should not, however, overlook the potential costs associated with this particular form of self-help. Taking the most extreme defensive stance, for example, people could effectively create a "white list" of other people from which they will accept messages in any public place. This would protect the listener from unwanted messages, but only by effectively isolating her from public communications she might have actually desired to receive.

It would thus seem that, as in the case of public captivity, audiences will mostly have to resort to self-help and other private means of avoidance when confronted with harassing expression in networked public places. According to some recent studies, this is apparently the way that Americans would prefer things. Survey results indicate that in many cases the public seems to prefer that norms rather than laws be used to regulate problematic expression.¹⁵⁶ One would expect that if given the option, these respondents might also prefer technological solutions to legal ones.

Virtual harassment and cyber-stalking are only two forms of harmful speech that may occur in networked public places. The examples demonstrate the common difficulty with protecting any of us from digitally conveyed expression in public places. Other dangerous or

155. See Steve Ranger, *This Text Will Self-Destruct in 40 Seconds*, SILICON, Dec. 12, 2005, <http://networks.silicon.com/mobile/0,39024665,39154995,00.htm> (describing a service in which email self-destructs within forty seconds of receipt).

156. See MARVIN AMMORI, *THE INFO. SOC'Y PROJECT*, YALE LAW SCH., PUBLIC OPINION AND FREEDOM OF SPEECH 22 (2006), available at http://research.yale.edu/isp/papers/ISP_PublicOpinion_fos.pdf.

harmful forms of expression, including “true threats” and “fighting words,” raise similar issues of pragmatics and proof.¹⁵⁷ Virtual threats and fighting words will not generally be witnessed events, in the sense that no material manifestation of them will occur and no public audience will experience them.

Moreover, these doctrines were developed with the imminence of real space and time in mind. Can one reasonably fear a threat delivered in a text message, with no further action taken? Can one invite a brawl through a text message?¹⁵⁸ Ultimately, as was true when stalking went online, it may be necessary to rethink or perhaps redefine the elements of these content categories to fit the new circumstances of networked public places. Or, alternatively, the networking of public places may provide further evidence that these categories are unworkable in a modern world in which the forms and mechanisms of communication are rapidly changing.

Nowhere are the effects of networking on space and time more likely to be felt than with regard to content in the category of “incitement to unlawful action.”¹⁵⁹ To constitute incitement, a communication must be “directed to inciting or producing imminent lawless action and . . . likely to incite or produce such action.”¹⁶⁰ What exactly does imminence indicate in networked public places?

The incitement doctrine, like many others, developed under conditions in which speakers and audiences were located in the same place. Wireless networking and pervasive computing erase spatial boundaries; these features can bring people together with remarkable speed and efficiency. As noted in Part II, mobile computing devices have the potential to facilitate assembly and collective action. The dark side of this, of course, is the power these devices have to facilitate collective acts of terrorism or other violence.¹⁶¹

On one hand, most Internet communications would seem to fail the imminence test. Internet communications can certainly lead to punishment for threatening speech, at least where tangible physical harm actually

157. See *Virginia v. Black*, 538 U.S. 343, 364-66 (2003); *Chaplinsky v. New Hampshire*, 315 U.S. 568, 572 (1942) (defining fighting words as those which “tend to incite an immediate breach of the peace”).

158. See JOHN HART ELY, *DEMOCRACY AND DISTRUST: A THEORY OF JUDICIAL REVIEW* 114 (1980) (describing fighting words as a “quite unambiguous invitation to a brawl”); see also Sanjiv N. Singh, *Cyberspace: A New Frontier For Fighting Words*, 25 RUTGERS COMPUTER & TECH. L.J. 283, 316-17 (1999) (examining psychological and physical injuries occasioned by online fighting words).

159. *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969) (footnote omitted).

160. *Id.*

161. For this reason officials must seriously consider whether providing wireless Web access on subway trains and other public facilities might facilitate future terrorist attacks.

occurs in material places.¹⁶² But in terms of incitement in particular, the nature of Internet communications is such that words on the Web are not generally delivered instantaneously to the audience.¹⁶³ Here, however, is one place where the intersection of material and cyber places may matter. The requisite imminence and risk of action may not have been present where a potential lawbreaker, sitting at his desktop in a pre-networked environment, posted a message on a website encouraging the like-minded to “move on City Hall.” But imminence and likelihood of harm may need to be calculated differently in a networked public environment. The networked speaker may be communicating from afar, while the threat on the ground from swarming and other coordinated activities may be both real and imminent. With constant accessibility to public Web access, co-actors would have instantaneous access to the speaker’s instructions and encouragements. Their mobility and access to shared information networks would significantly raise the risk of collective action.

The line between incitement and mere encouragement has always been somewhat hazy. Recent terrorism prosecutions appear to be pushing the limits of the imminence requirement under *Brandenburg*’s classic articulation of the incitement doctrine.¹⁶⁴ Suspects have been arrested prior to taking any substantial action toward perpetrating a crime, sometimes for little more than *discussing* their hatred for the United States or the possibility of some future attack.¹⁶⁵ New types of criminal activity like terrorism, coupled with new technologies like wireless networks and personal computing devices, need not necessarily change the definition of incitement. But they may well affect the delicate balance the doctrine requires officials and courts to maintain. The qualities of space and time, which help separate preemptive and illegitimate official acts and sanctions from lawful ones, will be less and less reliable indicators in networked places. Plausible arguments for stretching the scope of the imminence standard will arise as public places become networked.

The imminent melding of cyberspaces and material spaces will raise fundamental questions about doctrines developed to police expression that has until now been mostly material, physical, and visible. Personally harassing and offensive expression will likely have to be dealt with

162. See, e.g., *Planned Parenthood of the Columbia/Willamette, Inc. v. Am. Coal. of Life Activists*, 290 F.3d 1058 (9th Cir. 2002) (upholding damages award against organizations that published names, addresses, and other personal information relating to abortion providers on website).

163. See John P. Cronan, *The Next Challenge for the First Amendment: The Framework for an Internet Incitement Standard*, 51 CATH. U. L. REV. 425, 428-29 (2002) (noting “imminence” problem with regard to Internet communications).

164. See *Brandenburg*, 395 U.S. at 447.

165. See Eric Lipton, *Recent Arrests in Terror Plots Yield Debate on Pre-emptive Action by Government*, N.Y. TIMES, July 9, 2006, at A11 (reporting on recent terrorism plots and arrests).

through self-help mechanisms. Larger public safety threats may involve a reconsideration of concepts such as imminence and preemption. Policing incitements and threats that cannot be seen or heard will require ever more sophisticated surveillance capabilities and activities. As discussed below, this surveillance will raise substantial First Amendment concerns of its own.

D. *Protest: Assembly, Association, and Anticipatory Conformity*

Pervasive surveillance will make it possible for authorities to know of matters in advance, and thus to act preemptively. The technologies of surveillance are not only proliferating but becoming more and more powerful in terms of their capabilities. As a result we may no longer assume that we are blending into a public environment. Our activities, our associations, perhaps someday even our public *thoughts* may be discovered.¹⁶⁶

Public surveillance raises Fourth Amendment privacy concerns.¹⁶⁷ But there are serious First Amendment considerations as well. Depending on its ultimate form and scope, public surveillance may have substantial adverse effects on public expressive liberties. In terms of public expressive displays like protests and demonstrations, two general burdens will likely be imposed. First, there may be a chilling of *associative* rights. If assemblies are routinely watched and their activities recorded, it may be that speakers will be less likely to join in certain public causes. Second, there may be a chilling of *expressive behavior*. Sociologists, philosophers, and legal theorists have examined the phenomenon of “anticipatory conformity,” in which actors engage in self-restraining behavior when they believe they are being watched.¹⁶⁸ Given the nature of their expressive repertoires, political activists and other dissenters may disproportionately experience these effects.

Some have suggested that the mere existence of public surveillance cameras may violate the First Amendment.¹⁶⁹ Under current doctrine, however, there are substantial obstacles to such a claim. The most

166. If we follow the course taken by Great Britain, then it will one day be unusual *not* to have our public activities recorded. See CLIVE NORRIS & GARY ARMSTRONG, *THE MAXIMUM SURVEILLANCE SOCIETY: THE RISE OF CCTV* 42 (1999) (estimating that more than 300 cameras may film an individual in Britain each day).

167. Blitz, *supra* note 6, at 683. See generally Slobogin, *supra* note 5 (arguing that the Fourth Amendment requires regulation of public surveillance).

168. See Slobogin, *supra* note 5, at 242-44 (discussing research on anticipatory conformity).

169. See Blitz, *supra* note 6, at 696-98 (noting chilling effect on public urban speech activities and loss of anonymity); Slobogin, *supra* note 5, at 252-53 (“[O]ne might argue for a First Amendment right to be free of the inhibiting effects of camera surveillance in public unless the government can proffer some justification for it.”).

significant obstacle to a First Amendment claim based on the mere *existence* of public surveillance is *Laird v. Tatum*.¹⁷⁰ In *Tatum*, the Supreme Court held that a challenge to an Army covert surveillance program that tracked the activities of certain civil rights protest groups raised a non-justiciable controversy.¹⁷¹ The surveillance program's existence was not in dispute.¹⁷² But none of the alleged victims could demonstrate that they had suffered any cognizable injury as a result of being watched.¹⁷³ The Court acknowledged that a First Amendment violation might arise from something short of a direct prohibition on the exercise of First Amendment rights.¹⁷⁴ But the "chilling" effect recognized in prior cases, the Court said, involved exercises of governmental power that were "regulatory, proscriptive, or compulsory in nature, and the complainant was either presently or prospectively subject to the regulations, proscriptions, or compulsions that [the individual] was challenging."¹⁷⁵

Tatum suggests that any broadside by political groups or activists against general public surveillance programs is likely to fail.¹⁷⁶ In *Tatum*, authorities were attending public meetings and gathering information from news accounts.¹⁷⁷ Only the *means* of collecting information has changed. As in *Tatum*, only public information is being collected under known official surveillance programs. Of course, more serious concerns might be raised if specific groups or individuals were somehow targeted for public surveillance without sufficient cause.¹⁷⁸ The result might also be different if authorities were some day to link features of the network to access private Web or other electronic information about persons or groups who are gathering in public.

The mere *existence* of surveillance cameras situated in public places, however, would not seem to surpass *Tatum*'s jurisdictional hurdle, much less demonstrate a First Amendment violation. This will likely remain the

170. 408 U.S. 1 (1972).

171. *Id.* at 13-15.

172. *See id.* at 8.

173. *Id.* at 13-14.

174. *Id.* at 11.

175. *Id.*

176. Federal appeals courts have rejected several attacks on public surveillance programs based on *Tatum*. *See, e.g.,* Phila. Yearly Meeting of the Religious Soc'y of Friends v. Tate, 519 F.2d 1335, 1337-38 (3d Cir. 1975); Socialist Workers Party v. Attorney Gen. of the U.S., 510 F.2d 253, 255-57 (2d Cir. 1974).

177. *Tatum*, 408 U.S. at 6.

178. *See* Riggs v. City of Albuquerque, 916 F.2d 582, 583, 585 (10th Cir. 1990) (distinguishing *Tatum* where protesters alleged that targeted surveillance caused harm to reputation); *see also* Slobogin, *supra* note 5, at 255-56 (noting that some courts have distinguished *Tatum* where *targeted* surveillance affects membership or other specific group activities).

case so long as courts continue to view the harm or injury from pervasive surveillance as minimal and, what is more important, *non-regulatory*.

It is not difficult to imagine that pervasive surveillance at places like the National Mall may have serious chilling effects on public protest activity, both in terms of limiting associations and encouraging the anticipatory conformity of public expressive behavior. The same effect might be imagined in public squares and parks across the country. But imaginings are not concrete harms. What is required—if plaintiffs are to remain in court, and have a chance of success—is a much stronger showing that such chilling effects actually exist.¹⁷⁹

As the technologies of surveillance become more sophisticated, research on their expressive effects must keep pace. There is already a body of research examining the societal effects of pervasive surveillance. Many criminologists, urban geographers, and sociologists have concluded that public surveillance (a) does not serve to reduce crime, (b) excludes certain populations from public areas, and (c) reduces tolerance for “difference,” including unconventional (but not illegal) behavior.¹⁸⁰ These findings and conclusions raise substantial First Amendment concerns. At this point, however, there is insufficient research to convincingly demonstrate that constant surveillance amounts to a form of regulatory harm. It must be shown that the networked environment actually prevents or substantially discourages speakers and assemblies from engaging in public expressive activities. Even with such a showing, however, the government’s response will likely be that the threat of terrorism and other criminal activity is a compelling reason to put public areas under surveillance. Indeed, that concern has already caused some courts to loosen restrictions on political surveillance.¹⁸¹

There is little doubt that pervasive public surveillance will affect the exercise of public liberties. The present challenge is to demonstrate these effects concretely, in a manner that satisfies *Tatum*. We have a sociological expectation of blending in and avoiding constant scrutiny while in public places. Right now, however, we have no enforceable legal or constitutional right of this sort.

E. *Privacy: Identity, Thought, and Compulsory Speech*

Political activists and protesters will have a difficult time convincing courts of their right to avoid public scrutiny. What about the public

179. See Slobogin, *supra* note 5, at 245–46 (noting only a “small amount” of evidence has thus far been generated to prove the effect).

180. See *id.* at 248–49.

181. See *Alliance to End Repression v. City of Chicago*, 237 F.3d 799 (7th Cir. 2001) (removing some restrictions on surveillance); *Handschu v. Special Servs. Div.*, 273 F. Supp. 2d 327 (S.D.N.Y. 2003) (removing some restrictions on surveillance).

solicitor, pamphleteer, or solitary speaker? A speaker's right to communicate anonymously in public may be compromised by identity-exposing surveillance. Network-facilitated intrusions may someday make it possible for authorities to know a person's thoughts, for example by knowing what websites she has visited while in public areas or even, as technology becomes more sophisticated, by reading her face. Digitized environments may compel speakers to announce their identities and other information. Will any of these things violate the First Amendment?

Protection of one's *identity* is an aspect of the First Amendment's privacy guarantee. Recall that in *McIntyre v. Ohio Elections Commission*,¹⁸² the Supreme Court held that there was at least a limited right to communicate anonymously.¹⁸³ Given the power of today's surveillance technologies, it is certainly conceivable that in the future the right to anonymous pamphleteering could be violated in several ways. Cameras might reveal personal identifying information from distances of hundreds of feet.¹⁸⁴ As it develops, facial recognition technology may also reveal one's identity to authorities. In a future public environment, a speaker may be forced somehow to authenticate himself—by digital tags on his person or objects—before being permitted to enter a particular public place.

All of these things would disclose a person's identity to authorities, at times while she is engaged in protected speech. But *McIntyre* would only seem to protect identity in the hypothetical case of the exposed pamphleteer. The decision does not protect any generalized right of speakers to disguise or conceal their identities while in public.¹⁸⁵ Rather, it protects the right to *publish* one's views anonymously.¹⁸⁶ Identity is protected, in other words, not for its own sake but in connection with the act of publishing some message or view of the author. The author wishes to publish those views in such a manner that viewers remain unaware of her identity, whether for fear of reprisals or for expressive effect.¹⁸⁷

182. 514 U.S. 334 (1995).

183. *Id.* at 357; *cf.* Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Village of Stratton, 536 U.S. 150, 169 (2002) (invalidating ordinance that required door-to-door solicitors to disclose their identity).

184. See Slobogin, *supra* note 5, at 222.

185. See, e.g., Church of the Am. Knights of the Ku Klux Klan v. Kerik, 356 F.3d 197, 211 (2d Cir. 2004) (upholding New York's ban on wearing masks in public places).

186. See *McIntyre*, 514 U.S. at 342 ("The freedom to publish anonymously extends beyond the literary realm.").

187. See *id.* at 341-42. For these same reasons, courts have protected the rights of Internet speakers to maintain anonymity in connection with the publication of their views. See Blitz, *supra* note 6, at 704-05 (discussing cases and drawing analogy between public space anonymity and Internet anonymity); see also Lee Tien, *Who's Afraid of Anonymous Speech? McIntyre and the Internet*, 75 OR. L. REV. 117 (1996) (discussing cases that support giving First Amendment protection to online anonymous speech).

As long as governments do not regulate identity by prohibiting dissemination of anonymous messages, *McIntyre* would appear to provide no relief to those whose identity is merely exposed as a result of public surveillance. This does not mean that the loss of anonymity will have no effect on public expression and public life more generally. At this point in time, however, First Amendment conceptions of privacy do not encompass a *general* right to conceal one's identity while in public places.

More disturbingly, the networking of public places may also someday make it possible for authorities to intrude on the private *thoughts* of citizens. The First Amendment protects a private realm of thought, including what books we read, what websites we choose to visit, and what beliefs we hold.¹⁸⁸ Certain networking features will implicate this aspect of expressive privacy.

Municipal involvement in the operation of public WiFi systems may endanger this aspect of First Amendment privacy. Again, the experience of public libraries that provide Web access may provide some insight. Librarians have been vigorously resisting official requests made under the USA PATRIOT Act¹⁸⁹ for patron library records.¹⁹⁰ The librarians have been defending their patrons' right to access information without fear of governmental surveillance of their reading habits. They seek to protect patrons' First Amendment rights to free inquiry and thought.¹⁹¹

The libraries are well positioned, institutionally and as a matter of their basic mission, to resist such requests. Suppose, however, that a municipality providing or partnering with an Internet Service Provider to provide public WiFi receives credible information concerning a terrorist organization or an individual believed to be implicated in a terrorist plot. If the municipality is the sole provider of wireless Internet access, what will prevent it from monitoring or accessing the records of that organization or person? If it is providing access in partnership with a private service provider, will the provider feel pressured to turn over such information—in some cases without a subpoena? If the Web constitutes a "library" of information, records of what one is searching ought to be protected regardless of the place in which the search occurs—in the home,

188. *See* *Griswold v. Connecticut*, 381 U.S. 479, 482 (1965) ("The right of freedom of speech and press includes not only the right to utter or to print, but the right to distribute, the right to receive, the right to read and freedom of inquiry, freedom of thought . . .") (internal citations omitted).

189. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, 50 U.S.C.A. § 403-5d (West 2006).

190. *See, e.g.*, Alison Leigh Cowan, *U.S. Ends a Yearlong Effort to Obtain Library Records Amid Secrecy in Connecticut*, N.Y. TIMES, June 27, 2006, at B6.

191. *See id.*

in a library, or on a public bench.

A more literal interference with private thoughts may occur in fully networked public places. The First Amendment does not permit governments to punish anyone for merely *thinking* bad thoughts.¹⁹² Next generation facial recognition programs may offer a window into a person's private thoughts. Facial recognition software, which has been used at major sporting and other public events, maps the details and ratios of facial geometry using certain algorithms.¹⁹³ The most prevalent of these is the "eigenface," which is composed of "eigenvalues."¹⁹⁴ The current technology has substantial error rates.¹⁹⁵ But future generations of this technology will no doubt be more accurate in identifying individuals and reading their faces.

Suppose the technology existed to permit officials to canvass a crowd, focus on a specific person identified as a potential threat of whatever nature, and calculate his eigenvalues. To make the matter more concrete, suppose a paroled child predator appears at a public park where several children are playing.¹⁹⁶ Suppose further that the predator has done nothing in terms of approaching the children or otherwise acting on whatever impulses he may have. But his eigenvalues, captured on a public surveillance camera, reveal that he is so inclined.¹⁹⁷

Is there a basis for preemptively arresting the predator if these measures strongly indicate some fantasy or other invidious proclivity toward the children in the park?¹⁹⁸ Under current doctrine the answer would appear to be no.¹⁹⁹ The predator may be arrested for the *acts* he commits while in a public place, but not for what he merely happens to be

192. See *R.A.V. v. City of St. Paul*, 505 U.S. 377, 395-96 (1992) (invalidating ordinance that purported to punish racist thoughts); *Stanley v. Georgia*, 394 U.S. 557, 566 (1969) (noting that the state "cannot constitutionally premise legislation on the desirability of controlling a person's private thoughts").

193. Electronic Privacy Information Center, Face Recognition, <http://www.epic.org/privacy/facerecognition> (last visited Oct. 4, 2006).

194. See ANDREA SELINGER & DIEGO A. SOCOLINSKY, APPEARANCE-BASED FACIAL RECOGNITION USING VISIBLE AND THERMAL IMAGERY: A COMPARATIVE STUDY 8 (2002), available at http://www.equinoxsensors.com/publications/andreas_face.pdf.

195. See DUANE M. BLACKBURN ET AL., FACIAL RECOGNITION VENDOR TEST 2000 EVALUATION REPORT 14-22 (Feb. 16, 2001), available at http://www.frvt.org/dls/FRVT_2000.pdf.

196. The hypothetical is based on the facts of *Doe v. City of Lafayette*, 377 F.3d 757, 759-60 (7th Cir. 2004).

197. Malcolm Gladwell has provided an account of the work of psychologist Paul Ekman regarding facial signaling. See Malcolm Gladwell, *The Naked Face: Can You Read People's Thoughts Just by Looking at Them?*, NEW YORKER, Aug. 5, 2002, at 38, available at http://www.gladwell.com/2002/2002_08_05_a_face.htm.

198. See *Paris Adult Theatre I v. Slaton*, 413 U.S. 49, 67-68 (1973) ("The fantasies of a drug addict are his own and beyond the reach of government . . .").

199. See *id.*

thinking while there. Until now this matter has not been one of serious concern. Governments, after all, cannot read citizens' minds. But as one commentator has noted: "Current research blurs the boundary between biometrics and mind reading."²⁰⁰ Like our identities, our thoughts may be exposed in future networked environments. Technology will make thoughts more and more accessible to authorities.

Finally, speakers in networked public places may often be compelled *to speak* in the sense of identifying and authenticating themselves. Suppose, for example, that as a condition of access to some public place, the government requires that a machine must read a compulsory identification card. The First Amendment protects the right not to be compelled to express thoughts and beliefs against one's will.²⁰¹ The hypothetical compulsion here does not, however, compel the stating of any belief, creed, or thought. It is more akin to the sending of an administrative email, an act the Supreme Court recently found not to implicate the First Amendment's ban on compelled speech.²⁰² Such a system would be more akin to regulating conduct—in this case entry—than speech, thought, or belief.

The networking of public places will strain currently recognized rights to maintain speaker anonymity. It will facilitate the surveillance of records indicating private interests and preferences. It may ultimately expose the thoughts of public citizens. And it will compel authentication, perhaps constantly. Again, much will depend on how the technology develops and is used. The most that can be said at this point in time is that there are serious First Amendment privacy concerns lurking in the features of networked public places. Whether any of them will ripen into constitutional violations will ultimately depend on their sophistication and uses.

F. Press: "Citizen-Journalists" and Disclosures of Private Information

The networking of public places will also affect the reporting of news and the flow of information. These things are of course critical to core First Amendment values such as self-government and the search for truth.

In the traditional model, news was gathered and disseminated by major

200. Mitchell Gray, *Urban Surveillance and Panopticism: Will We Recognize the Facial Recognition Society?*, 1 SURVEILLANCE AND SOC'Y 314, 324 (2003), available at [http://www.surveillance-and-society.org/articles1\(3\)/facial.pdf](http://www.surveillance-and-society.org/articles1(3)/facial.pdf).

201. See *Wooley v. Maynard*, 430 U.S. 705 (1977) (holding that the state could not compel citizens to display the state motto on license plates); *W. Va. State Bd. of Educ. v. Barnette*, 319 U.S. 624 (1943) (invalidating compulsory flag salute for school children).

202. See *Rumsfeld v. FAIR, Inc.*, 126 S. Ct. 1297, 1308 (2006) (holding that compelling law schools to assist military employers with logistics of recruitment did not compel schools to speak).

news media outlets. Reporters at news desks and on the beat delivered information to a mostly passive public audience. Today, however, citizens have become increasingly involved in newsgathering and publishing. The Internet, of course, is the primary force behind this change. Weblogs at first supplemented and now appear to be displacing the traditional press as sources of information. The networking of public places will continue this trend. It will fill streets, parks, squares, and other public places with citizen-journalists. Citizen-journalists will be able to easily deliver the "live and on the scene" portion of the news that bloggers miss while at their desks. They will be able to go out in the "field," interview witnesses to events, and publish "reports" to an already growing number of Web clearinghouses.²⁰³

This trend toward citizen-journalism raises two important First Amendment issues. The first issue involves the very definition of "the press." There is at this moment a serious debate regarding whether those who contribute and post to Weblogs qualify as press under the First Amendment.²⁰⁴ This question has some important pragmatic implications. For example, if they are members of the press, bloggers would presumably be entitled to whatever privilege for withholding confidential sources the mainstream press possesses.²⁰⁵ In broader terms, although the press has few special privileges under the First Amendment, its status presents special considerations with regard to such things as prior restraints and the application of general laws to press interests.²⁰⁶ If nothing else, the mantle of the press may cause courts to more carefully scrutinize the limits on information gathering and publishing by citizen-journalists.

The Weblog now performs many of the same functions as major news media outlets in terms of informing the public, exposing governmental corruption, and providing public access to information on a broad array of issues of public concern.²⁰⁷ Whether by serving these functions bloggers

203. Of course, for these clearinghouses to become legitimate news sources there will have to be some means of measuring and ensuring accuracy and reputation.

204. See Mary-Rose Papandrea, *Citizen Journalism and the Reporter's Privilege*, 92 MINN. L. REV. (forthcoming 2007) (examining bloggers and other disseminators of information).

205. But see *Branzburg v. Hayes*, 408 U.S. 655 (1972) (declining to explicitly recognize such a privilege). Many states have journalist shield laws. See, e.g., CAL. CONST. art. 1, § 2(b). One court has recently held that a state law extends to Weblogs. See *O'Grady v. Super. Ct. of Santa Clara County*, 44 Cal. Rptr. 3d 72, 105 (Cal. Ct. App. 2006) (holding that California journalist's privilege extends to Weblog). Courts could also create a journalist's privilege under the common law. See *In re Grand Jury Subpoena, Judith Miller*, 438 F.3d 1141, 1156-57 (D.C. Cir. 2006) (declining to create a common-law journalist's privilege, in part owing to the difficulty of deciding whether bloggers and other citizen-journalists would be entitled to protection).

206. See *N.Y. Times Co. v. United States*, 403 U.S. 713, 714 (1971) (per curiam) (invalidating injunction prohibiting publication of Pentagon Papers).

207. See Linda L. Berger, *Shielding the Unmedia: Using the Process of Journalism to Protect*

are entitled to constitutional protection for sources or other press privileges is an interesting question.²⁰⁸ If they are, then one must ask whether “the press” continues to convey anything truly meaningful in constitutional terms. After all, as one commentator has said: “When everyone can be a member, the club can no longer promise special treatment.”²⁰⁹

The networking of public places will contribute to the blurring of the line between members of the public and members of the press. Sophisticated means of information gathering and publishing will be available to more and more citizens. Like bloggers, on-the-ground citizen-journalists will likely claim First Amendment privileges and protections. In *United States v. Wolf*, a freelance journalist was jailed for refusing to turn over to a grand jury footage of a political protest in which anarchists were suspected of vandalizing a police car.²¹⁰ The Ninth Circuit recently refused to recognize a journalist’s privilege for withholding the video footage.²¹¹

Courts will increasingly be called upon in cases like *Wolf* to determine not only the scope of constitutional privileges but also the classes of persons entitled to claim them. If “the press” is to retain any constitutional meaning at all, then not every citizen armed with a recording device and an Internet connection can be considered a member. Among other things, the extent to which extending privileges and other protections to millions of citizen-journalists would undermine law enforcement interests surely counsels against expanding the definition too far. And the ordinary citizen is not likely to be cultivating sources to facilitate the flow of sensitive information. She is much more likely to be recording events as they occur on the ground. She will be subject to no editorial oversight or professional standards.²¹² She will be primarily observing, with the additional and often merely incidental capabilities of recording and publishing. She will, in

the Journalist’s Privilege in an Infinite Universe of Publication, 39 HOUS. L. REV. 1371, 1378 (2003) (noting the merger of citizen and journalist functions).

208. See, e.g., Laura Durity, *Shielding Journalist-“Bloggers”: The Need to Protect Newsgathering Despite the Distribution Medium*, 2006 DUKE L. & TECH. REV. 11, ¶ 36-38 (arguing in favor of functional definition of “journalist” that would cover “journalists who use blogs as a mere distribution device for their work”); see also Papandrea, *supra* note 204 (arguing that every person who disseminates information to the public should be presumptively entitled to invoke the reporter’s privilege).

209. Berger, *supra* note 207, at 1378.

210. *In re Grand Jury Subpoena*, Joshua Wolf, No. 06-90064 (N.D. Ca. July 21, 2006) (granting Order to Show Cause), available at <http://joshwolf.net/grandjury/NEW/osc-contempt.pdf>; see also Bob Egelko, *Cameraman Jailed for Not Yielding Tape*, S.F. CHRON., Aug. 2, 2006, at A1.

211. See *Wolf v. United States*, No. 06-16403, 2006 WL 2631398, at *1 (9th Cir. Sept. 8, 2006) (upholding contempt citation).

212. See Anne Flanagan, *Blogging: A Journal Need Not a Journalist Make*, 16 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 395, 415-17 (2006) (urging use of code of ethics as one standard for determining who qualifies as a “journalist”).

short, remain more citizen than journalist.

The second First Amendment issue relates to what all of these citizen-journalists shall be permitted to report about. Some of what transpires in public places consists of private facts and moments. As discussed earlier, we expect, at least some of the time, to blend into public places. If we cannot, this may affect public expressive activities. The question here is whether there are any limits on fellow citizens' efforts to report and publish private facts in public settings.

The Supreme Court has been highly protective of the right to publish information, so long as it is lawfully obtained and of some interest to the public. In *Florida Star v. B.J.F.*,²¹³ the Court held that a newspaper could not be punished under state law for truthfully publishing the name of a rape victim it had obtained lawfully.²¹⁴ Even this very personal fact was considered "newsworthy."²¹⁵

The constitutional standard announced in *Florida Star* is in conflict with the privacy tort known as "publicity given to private life."²¹⁶ Indeed, as Justice White stated in his dissent in *Florida Star*, the decision effectively "obliterated" the tort.²¹⁷ The standard of public significance or "newsworthiness" ultimately protects very little of our private lives from public disclosure. The standard is designed to permit the broadest gathering and dissemination of information. This is a salutary thing, of course, in terms of First Amendment values. Indeed, some have suggested that the public disclosure privacy tort is wholly at odds with these basic values.²¹⁸ If the tort is interpreted too broadly, it will likely chill speech and thus interfere with the flow of information to the public.

When everyone becomes a gatherer and disseminator of news, however, then *everything* becomes to some degree a matter of public significance. The networking of public places, which will be filled with citizen-journalists, will make us all increasingly newsworthy subjects.²¹⁹ If the tort of public disclosure of private facts was not already dead, then

213. 491 U.S. 524 (1989).

214. *Id.* at 541.

215. *Id.* at 533.

216. RESTATEMENT (SECOND) OF TORTS, § 652D (1977).

217. *Florida Star*, 491 U.S. at 550 (White, J., dissenting).

218. See Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 362 (1983) (arguing that the "private-facts tort" threatens to chill speech and should be abandoned).

219. Politicians, who are already newsworthy subjects, are finding that the networking of public places is altering the political climate and public politicking. See Ryan Lizza, *The YouTube Election*, N.Y. TIMES, Aug. 20, 2006, § 4, at 1 (discussing incident in which Senator George Allen, the Virginia Republican, was caught on tape at a campaign event using a racial slur; the video appeared on YouTube, a videosharing website).

the networking of public places will surely contribute to its passing.²²⁰ Citizen-journalists, like traditional reporters, will have few limits with regard to what is within their legitimate domain of reportage. This may further discourage, among other things, public expressive activity.²²¹

We may well wish to have some legal recourse in networked places crawling with camera-toting citizen-journalists. We certainly must expect to be observed in public. But that does not mean we expect that our every move will be recorded by citizen-journalists.²²² The threat of tort liability might preserve at least some measure of private, anonymous life in public places. To this end, Professor Andrew McClurg has suggested that the privacy torts be expanded to include some right to "public privacy."²²³ He argues that a tort action is needed for what he calls "public intrusions."²²⁴ As support for the recognition of this tort, he cites two factors—an increasingly aggressive media and advances in video and other surveillance and recording technologies.²²⁵

Although the matter is quite close, the First Amendment balance seems best struck in favor of recognizing such a tort. There must of course be protection for citizen-journalists' gathering and disseminating of matters of legitimate public interest.²²⁶ As noted earlier, protesters who videotape public events can effectively challenge official accounts of these events. But when the matter recorded and published is one of wholly private interest—who one embraces, or meets with, or what books or magazines one reads, for example—then there should be some protection against intrusion even if the activity occurs in public. Taking the larger First Amendment view, such protection will help to ensure that there is continued presence in and use of public places. There are already many factors that work against this presence and use, including pervasive *official* surveillance programs.²²⁷ Citizen-journalists should not be permitted to contribute to these constraints by indiscriminately recording and

220. For an argument that the tort was never terribly effective at protecting private information, see Andrew J. McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality*, 74 U. CIN. L. REV. 887, 903-04 (2006).

221. See *supra* notes 166-81 and accompanying text.

222. See RESTATEMENT (SECOND) OF TORTS § 652D, cmt. C (discussing highly offensive publicity and noting that a citizen must tolerate "more or less casual observation"); *id.* illus. 10 ("A publishes, without B's consent, a picture of B nursing her child. This is an invasion of B's privacy."); see also *id.* § 652B cmt. C, illus. 7 (describing the publication of a young woman's picture, taken at a public "Fun House," showing her skirt over her head, as an invasion of privacy).

223. See 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, 1055 (1995) (proposing adoption of tort of public intrusion on privacy).

224. See *id.* at 1010-25.

225. See *id.*

226. See *id.* at 1082-85 (discussing public interest factor).

227. See *supra* Part II.B.2 (discussing pervasive official surveillance).

publishing private moments in public places that are not newsworthy.

The First Amendment effects produced by the networking of public places will be both wide and deep. Even the ongoing controversy over who constitutes “the press” will be affected to some degree. Pervasive computing and constantly available Web access will turn everyone into a potential citizen-journalist capable of filing reports from the “field.” We ought to ensure that when all of this taping and recording captures private moments and events, there will be some recourse in tort law. The First Amendment interests in continued use of public places outweigh the right of the citizen-journalists to “report” news that is of no legitimate public interest.

IV. NETWORKED PUBLIC PLACES AND DEMOCRATIC VALUES

Although it is important to consider the effect networked places may have on individual and collective First Amendment rights, there are much larger issues lurking in the steady progression toward networked public places. As Professor Julie Cohen recently reminded us, cyberspace and other technologies do not exist or operate in a spatial vacuum.²²⁸ These things affect the lived, embodied spaces of real people.²²⁹ Professor Cohen is surely correct that “[c]yberspace is part of lived space.”²³⁰ As the foregoing discussion shows, this is now quite literally true. Clouds, cameras, and computers are altering the public expressive environment. They are affecting how we interact, who we interact with, and what information is at hand as we live and experience public places.

Networking will bring fundamental changes to urban and suburban landscapes. We must assess not only expressive *rights*, but expressive *values* as well. We must ask what sort of *lived* spaces networked places will ultimately be.²³¹ What effect will spatial networking have on the ability of public places to serve critical First Amendment values, such as those related to self-government? To examine this impact effectively we must consult the work of geographers and sociologists as well as constitutional scholars. Although it is too infrequently acknowledged, what these other disciplines have to say about public places is central to the constitutional considerations at hand.

228. See Cohen, *supra* note 4, at 3-4 (asserting that theories of cyberspace must take into account the “situated experience of cyberspace users and the complex interplay between real and digital geographies”).

229. *Id.* at 4.

230. *Id.*

231. See Blitz, *supra* note 6, at 682 (noting that surveillance of urban spaces may transform cities into small towns); Kang & Cuff, *supra* note 4, at 119 (“As we percolate the physical environment, we intentionally or inadvertently redesign the public sphere. In doing so, we will either catalyze or inhibit its primary functions.”).

A. *Public Places and the Public Sphere*

An initial point of clarification is necessary. In determining what effect networking will have on public expressive life, we must concretize matters by clarifying the relevant places under consideration. "Public places" is a phrase that obviously denotes a large geographic canvas. This Article has been concerned with public *expressive* places in the broadest sense, from sidewalks to malls to street corners. These places make up what I have elsewhere referred to as an "expressive topography"—the public space potentially available for expressive activities.²³² These places are all to one degree or another becoming networked places.

My use of "public place" is narrower than the concept of the "public sphere."²³³ Professors Kang and Cuff have analyzed the effect of one particular aspect of the networked environment—pervasive computing—on the public sphere.²³⁴ As they conceive it, this sphere "connotes the comprehensive intermingling of spatial and social terrains."²³⁵ The public sphere, they say, is an open space of interaction and exchange, a shared space separate from the "intimate, protected, and familiar" private sphere.²³⁶ This sphere is much broader than public places. Indeed, Kang and Cuff note that the public sphere extends to such places as movie theatres, laundromats, even *traffic jams*.²³⁷

To analyze the effects of pervasive computing on the public sphere, Professors Kang and Cuff chose as their paradigmatic spatial example the shopping mall, a place that illustratively and effectively combines elements of community and commerce.²³⁸ They appear to have chosen the mall for two general reasons. First, they note that "in many urban environments, malls are arguably what our public spaces have become."²³⁹ This is unfortunately true, insofar as public places now facilitate commerce more than any other form of interaction. Second, the mall was chosen as a paradigm because it is a place where people can generally be found. As Kang and Cuff say, their aim was to be "practical and look at the spaces where people actually are, not where academics long for them to be."²⁴⁰

232. See Zick, *Space, Place, and Speech*, *supra* note 33, at 440.

233. See generally RICHARD SENNETT, *THE FALL OF PUBLIC MAN* (1976) (discussing concept of the public sphere).

234. Kang & Cuff, *supra* note 4, at 116.

235. *Id.*

236. *Id.*

237. *Id.* at 116-18 (discussing the "public sphere").

238. *Id.* at 119 (adopting the shopping mall as the relevant application).

239. *Id.*

240. *Id.* at 120; see, e.g., Jennifer Niles Coffin, Note, *The United Mall of America: Free*

The focus on the public sphere generally, and the mall in particular, is both too broad and too narrow. It is too broad if one is asking, as this Article does, what effect spatial networking will have on *expressive* values. Many of the places in the public sphere, including laundromats and traffic jams, have no connection at all to such values. Malls as a class of property are not presently considered expressive fora.²⁴¹ The shopping mall in particular is an example of what I have elsewhere called, borrowing a term from geographers, an expressive “non-place”—a space where expressive culture is discouraged or prevented from developing.²⁴² To be sure, as Kang and Cuff note, urban social critics have long lamented the “mall” of public place.²⁴³ But to an extent this begs the question: What functions *ought* our public places serve? As well, whether or not academics wish it so, people in fact do remain on the streets, in the parks, and in public squares. They continue to rely on these places, and others, to exercise public expressive liberties. We ought to ask how networking technologies will affect expressive activity in such places.

The paradigm we should adopt in order to address expressive values is not *a* mall, but something more akin to *the* (National) Mall.²⁴⁴ For purposes of the discussion that follows, let us take as our paradigm place not the shopping mall but the public park or public square. These are the sorts of places that are most critical in terms of engendering civic republicanism and a sense of democratic community.²⁴⁵

What speech activity will occur or be possible in these places once they become networked? Who will actively participate, and by what means? How democratic and facilitative of self-government will networked public places actually be? What steps might be taken to ensure that public

Speech, State Constitutions, and the Growing Fortress of Private Property, 33 U. MICH. J.L. REFORM 615, 617-18 (2000) (noting the multiple functions of the modern shopping mall).

241. See *Hudgens v. NLRB*, 424 U.S. 507 (1976) (holding that labor picketers had no right to demonstrate at a shopping center); *Lloyd Corp., Ltd. v. Tanner*, 407 U.S. 551 (1972) (holding that protestors of the Vietnam War had no right to distribute handbills in shopping center).

242. See Zick, *Space, Place, and Speech*, *supra* note 33, at 480 (discussing mall spaces as part of the expressive topography). As Kang and Cuff note, in the mall “[p]eople-watching, not self-governance, may be what is on the agenda.” Kang & Cuff, *supra* note 4, at 117 (footnote omitted).

243. See, e.g., Margaret Crawford, *The World in a Shopping Mall*, in VARIATIONS ON A THEME PARK: THE NEW AMERICAN CITY AND THE END OF PUBLIC SPACE 3 (Michael Sorkin ed., 1992).

244. Kang and Cuff would no doubt object that theirs is the more practical paradigm, because they “look at the spaces where people actually are, not where academics long for them to be.” Kang & Cuff, *supra* note 4, at 120. But people definitely remain on the streets, in the parks, and in public squares. They go to these places, and others, to exercise public expressive liberties. That they may do so less often than they go to a shopping mall is beside the point. It may beg the question whether public spaces that were more conducive to expression would be less sparsely populated.

245. See MICHAEL J. SANDEL, *DEMOCRACY’S DISCONTENT: AMERICA IN SEARCH OF A PUBLIC PHILOSOPHY* 335-36 (1996) (commenting on the connection between New Urbanism projects focusing on the centrality of public places, community, and civic republicanism).

expressive values will endure in the public places of the future? To answer these questions we must first have a better sense of the expressive functions that public places ideally might serve.²⁴⁶

B. *The Democratic Functions of Public Places*

Public places substantially influence the nature and character of public citizenship.²⁴⁷ Their architectures (material and otherwise), the degree of freedom of access to them, and the nature of public interaction within them, mark the boundaries of our public liberties. To the extent that our public places are open and vibrant, they have the capacity to facilitate citizens' claims to identity, create breathing space for democratic participation and self-governance, and lend transparency to public expression and democratic governance. To the extent that use of such places is discouraged by spatial networking, these critical democratic functions are diminished. To be quite clear, what follows is very much a description of an *ideal* state of affairs. I do not contend that parks, squares, and other expressive places currently serve the highlighted functions, or even that they serve them very well. My general point is that we should not build a networked environment that further undermines these functions.

1. Place and Identity

Democratic citizenship involves living among others in a polity. Regardless of how often we may retreat to private enclaves, citizenship still requires some degree of public presence. As geographers have noted, the presence of an individual or group in public places is itself a claim to acceptance.²⁴⁸ It is important that all citizens have an equal opportunity actively to participate in expressive activities in public places.

Material public places, as noted in Part II, serve a leveling or equalizing function in this regard. The causes of "little people" find a voice there.²⁴⁹ The recent nationwide immigrant protests made a

246. I do not contend that public places currently serve these functions, nor that they do so effectively in most cases. I wish to inquire whether the networking of public places might further undermine these ideal functions, and if so, how.

247. See Blitz, *supra* note 6, at 710-11 (discussing importance of urban places like parks and streets to First Amendment rights and public experience).

248. See generally DON MITCHELL, *THE RIGHT TO THE CITY: SOCIAL JUSTICE AND THE FIGHT FOR PUBLIC SPACE* (2003) (noting how presence in place constitutes a claim to acceptance as part of community); see also Nancy Fraser, *Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy*, in HABERMAS AND THE PUBLIC SPHERE 109, 109-42 (Craig Calhoun ed., 1991) (noting that groups traditionally excluded from the public sphere formed counterpublics).

249. See *Martin v. City of Struthers*, 319 U.S. 141, 146 (1943) (referring to the common

quintessential identity claim in this fashion.²⁵⁰ By assembling in the streets and expressing themselves there, immigrants communicated a clear message: “We are here, and we are not going anywhere.” Their demonstrations and other activities sparked a national conversation about the nation’s immigration policies.²⁵¹ The situation bears some resemblance to the identity claims civil rights protesters made in the 1960s when they took to the streets, occupied public buildings, and staged sit-ins. They too were arguing for inclusion in a democratic community. Their very presence in public places symbolized their right to exist and to be counted as members of the polity.

If access to public places indicates acceptance, then exclusion or substantial displacement conveys denial of one’s public identity. This is sometimes a matter of social justice, as when the poor and homeless are ejected from substantial urban areas or harassed through aggressive enforcement of vagrancy laws.²⁵² Unfortunately, class biases persist in today’s public square. Officials can be overzealous in their efforts to preserve public norms of order and tranquility. For example, a federal appeals court recently invalidated a Los Angeles law permitting the arrest and conviction of the homeless for merely being—standing, sitting, or sleeping—in certain public places.²⁵³ The court held, in essence, that authorities cannot simply ban the public existence of an entire class of people.²⁵⁴

Public places are symbolic of equality, acceptance, and political community. They are open to all on an equal basis, regardless of social or economic class. To exclude someone, either directly or indirectly, from participation in public life is a derogation of a fundamental claim to public identity. Many forces negatively affect public claims of civic identity. Among these are the increasing trend toward privatization of public places, gender- and race-based public harassment, and a variety of legal regulations of the places where expression may occur.²⁵⁵ We must ask what further impact the networking of public places might have on public presence, participation, and identity claims.

people as “little people”).

250. See Sheryl Gay Stolberg, *After Immigration Protests, Goal Remains Elusive*, N.Y. TIMES, May 3, 2006, at A1 (describing protests and recent social activism of immigrants).

251. See *id.*

252. For a thorough examination of the social justice implications of access to public places, particularly claims of the homeless, see generally MITCHELL, *supra* note 248.

253. See *Jones v. City of Los Angeles*, 444 F.3d 1118, 1138 (9th Cir. 2006) (invalidating ordinance on Eighth Amendment grounds).

254. *Id.*

255. See Zick, *Speech and Spatial Tactics*, *supra* note 7, at 598-604; Zick, *Space, Place, and Speech*, *supra* note 33, at 442, 497.

2. Place and Self-Governance

In addition to facilitating identity claims, public places serve fundamental self-governance functions.²⁵⁶ They provide critical breathing room in which speakers can approach, speak to, and attempt to persuade audiences.²⁵⁷ In the material marketplace conversations with other public citizens take place, petitions are signed, leaflets and pamphlets are distributed, signs are carried and posted, parades and protests are staged. The people practice self-governance in public places.

Consider a place like the National Mall. The Mall is a deeply inscribed public place—sacred ground, one might say, insofar as self-governance is concerned. The condition of this place matters deeply in terms of shared national First Amendment values. Traditionally, speakers and audiences have gathered here and in other public places with some confidence that authorities were not tracking their every movement and utterance. This created open space for protest and dissent. But in a broader sense it also created a setting for democratic participation of all sorts. Public places have traditionally been part of a democratic commons, not militarized grids under constant surveillance by public and private devices.

It is not merely the character of these places but the manner in which people are able to interact while there that determines the scope of self-governance. Fundamentally, self-governance requires that listeners hear and audiences see speakers who attempt to convey messages. One of the principal advantages of physically emplaced expression, as opposed to the many burgeoning forms of virtual communication, is its ability to jar an audience, to force it to heed the messenger (if not the message). Jehovah's Witnesses, labor activists, anti-war protesters, suffragists, feminists, and civil rights proponents have all relied on the tangibility and physicality of public places and public expression to further their causes. They have understood, as many still do, that effective speech sometimes entails

256. See ALEXANDER MEIKLEJOHN, *FREE SPEECH AND ITS RELATION TO SELF-GOVERNMENT* 14-16, 24-27 (1948) (elaborating a self-governance theory of expression); Kent Greenawalt, *Free Speech Justifications*, 89 COLUM. L. REV. 119 (1989) (discussing the idea of the "marketplace" and other free speech justifications).

257. To be sure, some have long doubted the salience of outdoor expressive activities like protest, solicitation, and pamphleteering. See, e.g., Owen M. Fiss, *Why the State?*, 100 HARV. L. REV. 781, 793-94 (1987) (arguing that the lack of locality and economic realities undermines the effectiveness of traditional public expression). A massive societal centralization has undermined the formation of community and the local conditions under which public expression might thrive. See generally SANDEL, *supra* note 245, at 205-08. Legal limits often undermine public expression. And today communicative outlets continue to proliferate on the Web and elsewhere. Although each of these things no doubt affects the incidence and effectiveness of public expression, people continue to seek public expressive space for their causes. Even in the virtual era, or perhaps especially so, people seek the physical and tangible.

interfering with the settled expectations of the unwilling or undecided public audience. Public places cannot serve fundamental participatory functions unless these conditions can regularly be met.

In addition to facilitating identity claims, public places are also pragmatic proving grounds for public speakers and audiences. They are, or at least have been, spaces for public interaction. Whether or not speakers have persuaded listeners, public places have provided them the opportunity to do so. Public self-governance depends upon the continued existence of such opportunities.

3. Place and Transparency

As noted in Part II, one of the defining characteristics of expression in material public places is its visibility and transparency. Public places serve two critical transparency functions. They assist speakers in making identity claims and facilitate public participation and self-governance.

First, because it takes place in the open, material public expression can be seen and heard by others occupying the same places. Unlike, say, lobbying and other forms of private attempts at political persuasion, public expression is part of a public record. The public audience can witness the speech of marginal groups. It can come to know and recognize a cause. The public can assess the look and feel of speakers. How disgruntled or angry is this group? Does it represent a potential threat to safety? Do I want to support its cause? For the speaker, public displays can attract media attention and public sympathy, expand participation in a movement or cause, and signal support for that cause to public officials.²⁵⁸ The transparency, or visibility, of public expression can create positive cascades in terms of public support, publicity, or policy change.²⁵⁹

Second, official regulation of public expression has itself tended to be visible and transparent. As the recent controversy regarding the National Security Agency's wiretapping program demonstrates,²⁶⁰ the degree of regulatory transparency affects public perceptions of the legitimacy of government. Traditionally, in material public places we have been able to see the tactics police are using to restrict public speakers and public assemblies. The public becomes a witness to these things. We are thus in a position to determine for ourselves whether official tactics respect basic

258. See, e.g., Susanne Lohmann, *A Signaling Model of Competitive Political Pressures*, 7 *ECON. & POL.* 181 (1995) (analyzing policy impact of public protests on congressional voting).

259. It can, of course, also create negative cascades, as when protests are violent or destructive.

260. See John Markoff, *Questions Raised for Phone Giants in Spy Data Furor*, N.Y. TIMES, May 13, 2006, at A1, A13 (reporting on fallout from domestic surveillance program). A district court recently invalidated the NSA surveillance program on First and Fourth Amendment grounds. See *Am. Civil Liberties Union v. Nat'l Sec. Agency*, 438 F. Supp. 2d 754, 782 (E.D. Mich. 2006).

civil liberties. Regulation of public places is among the very few instances in which transparency of this sort exists.

A vast amount of expression has recently migrated to the Internet. As it continues to go there, concerns continue to arise with regard to the transparency of governmental efforts to monitor expression in cyber-places. This is so because neither the speech on the Web nor its regulation is particularly transparent. The speech there is read and not witnessed and experienced by the public and the media. It is thus more critical than ever that we preserve public spaces that are both transparently experienced and regulated.

C. The Networked Public Citizen

The networking of public places will do more than raise some interesting First Amendment issues. It will substantially affect the First Amendment values that might ideally be served by public places. This section examines the effects networking will have on public expression and more generally, civic life, in public places. The final section offers some modest proposals that may help preserve the critical functions of public places.

1. Populated Places and the Public Digital Divide

Of course, public places cannot serve any particular function unless they are sufficiently visited and used. Until recently, maintaining network connectivity in public spaces faced substantial barriers. Online access was primarily available only in the private sphere.

Municipal wireless projects will turn entire cities and regions into hotspots. Access to information and communications technologies will burgeon even in currently underserved rural areas, further reducing the digital divide. In vast urban and suburban areas, citizens will no longer be limited to private areas when they wish to access the Internet. Concepts like online and offline will thus continue to lose relevance, at least for many citizens, as public places become networked. For those with access to the latest technologies, information will flow more freely everywhere.

This networking may have the salutary effect of increasing Americans' use of public places. It will also likely increase their use of mobile technologies in those places.²⁶¹ As some have noted, American citizens have been less likely than citizens in other countries to utilize mobile

261. The public library experience is again somewhat analogous. The obvious concern of public libraries as we entered an information age was how to remain vibrant, or even relevant, places for the consumption of information now delivered over networks rather than on shelves. By providing Internet access, public libraries not only helped to close a digital divide, but they also ensured that the library would remain a critical community space.

communications technologies in public places.²⁶² One suspected reason for this cultural divide is that in this country we have vast areas of private space—in our homes, our workplaces, and elsewhere—in which to engage in expression and interaction. It may also be the case that until now, our public network connections have been too weak to support robust use of the latest technologies in public areas. As clouds appear and networks are strengthened, we may expect to see many people personally computing and communicating in public places.

Those who study urban and suburban geographies might initially be encouraged by this prospect. Indeed, the basic agenda of “new urbanist” scholars and activists is to revive common spaces like parks and squares as centers of interaction and community-building.²⁶³ These theorists generally believe that by widening suburban sidewalks, planning communities around central public places, and cutting back single-use zoning, civic interaction can be greatly facilitated.²⁶⁴ Widely available wireless connectivity may provide citizens with a reason to remain in public places.

Of course, mere public presence is not the primary goal. New urbanists and other public place activists envision public places that promote encounters among citizens from different backgrounds, races, and ethnicities.²⁶⁵ Public expression is most vibrant when a variety of speakers engage in a variety of speech forms. But this raises the question: Who will the networked public citizen be? And whose identity claims will be most fully on display in newly networked parks and squares?

The networking of public places may have the unintended negative effect of creating new classes of haves and have-nots. A *public* digital divide may develop between technologically literate groups and the still publicly disconnected.²⁶⁶ The networked environment will become more and more facilitative of digital communication. Indeed, it may render access to digital technologies critical to public participation. Thus, public places may become more foreign and alienating locales for those unable to use the available, ubiquitous technologies.

262. Cf. RHEINGOLD, *supra* note 87, at 157-58 (describing the Phillippines’ smart mob’s extensive use of mobile technology).

263. See, e.g., Jerry Frug, *The Geography of Community*, 48 STAN. L.REV. 1047, 1089-94 (1996) (describing in general terms new urbanism principles).

264. *Id.* at 1092.

265. Much of this agenda dates back to the 1960s, when activists like Jane Jacobs stressed the importance of architecture to urban communities. See generally JANE JACOBS, *THE DEATH AND LIFE OF GREAT AMERICAN CITIES* (1993) (discussing architecture and its effect on urban communities).

266. For the status of the digital divide in the United States, see generally U.S. DEP’T OF COMMERCE, *FALLING THROUGH THE NET: TOWARD DIGITAL INCLUSION* (2000), available at <http://search.ntia.doc.gov/pdf/fttn00.pdf> (discussing increasing digital divide even while Internet access rises).

Wireless clouds and pervasive personal computing may even alter the socially acceptable uses of public places. Publicly online citizens may seek to enforce a norm of quiet computing that suppresses noisier forms of expression available to still-offline citizens. If they cannot enforce that norm, there is a danger that public "Netizens" may retreat back into their homes and other private spaces.

The transition to networked public places may affect the democratic functioning of places in ways that are not immediately apparent. Constant connectivity may bring people into the public square. But not everyone will be able to participate equally. New digital divisions and contests over appropriate behavioral norms in networked places may arise. The still-offline citizen may become further alienated, disengaged, and displaced in public, while the networked citizen's claims and displays may be increasingly privileged.

2. The People—Disconnected

Even if the people are drawn into public places, we must ask what sort of expressive activity will take place there. What sorts of claims, displays, and communication will occur? To serve identity, self-governance, and transparency functions, networked places must facilitate not only commercial and recreational interaction but more substantive public communication as well. But will they?

As noted in Part II, the networking of public places will provide greater opportunities for social networking.²⁶⁷ These networks will become more and more sophisticated. This should facilitate spontaneous assemblies in public places. Networked public assemblies, protests, and demonstrations should be smarter than ever before, at least for those with access to up-to-date technologies.

Even if this transpires, however, protests and demonstrations constitute only a small fraction of the public expressive culture. Ideally, public places ought to facilitate spontaneous interactions and speech claims of all sorts, everything from solicitation to petitioning to begging.²⁶⁸ Networked public places are not likely to do so, however. What we are more likely to see in networked public places is an increasingly *disconnected* populace.²⁶⁹

Among the connected, Web access carried over public networks on

267. See *supra* notes 85-92 and accompanying text.

268. See Blitz, *supra* note 6, at 686 (noting the particular importance of urban spaces to provide "opportunities for giving speeches to large crowds, for confronting strangers with ideas they may find unfamiliar or provocative, or for speaking or gathering information in the anonymity of the crowd").

269. See Kevin Robins, *Foreclosing on the City? The Bad Idea of Virtual Urbanism*, in *TECHNOCITIES* 34, 34-59 (John Downey & Jim McGuigan eds., 1999) (criticizing idea that one can restore a sense of community by building virtual communication networks).

pervasive mobile devices will increase the phenomenon known as “absent presence.”²⁷⁰ As sociologists and urban geographers have noted, people are becoming increasingly disconnected from events in material places.²⁷¹ This distance has serious First Amendment implications in terms of the identity, self-governance, and transparency functions of public places.

Networked public citizens, their eyes cast downward and ears filled with audio devices, may not see or hear messages other than those transmitted into their personal bubbles.²⁷² They will not see, hear, or experience a range of identity claims. They will be more inclined—and more able—to simply ignore solicitors, proselytizers, beggars, and other marginalized speakers. In addition, self-governance requires exposure to speakers and messages one does not agree with and may even be initially unwilling to engage.²⁷³ But the networking of public places will decrease chance encounters with unwanted messages.²⁷⁴

Speech in networked public places will also be less and less transparent. Wireless clouds and pervasive personal computing in public places will affect the very aesthetics—the look, feel, and experience—of public expressive activity. Formerly private communication forms like email and text messaging will proliferate, while tangible and face-to-face communication will continue to fade from public venues. Networking features and practices will alter even the expressive noise of public places.²⁷⁵ Public parks and squares will resemble offices and other private spaces of work and recreation.

The new urbanist philosophy suggests that if you build wider streets and more inviting spaces, people will come.²⁷⁶ People may indeed populate

270. See Cohen, *supra* note 4, at 36 (discussing absent presence, or what is sometimes referred to as “present absence”); see also Kenneth J. Gergen, *The Challenge of Absent Presence*, in PERPETUAL CONTACT: MOBILE COMMUNICATION, PRIVATE TALK, PUBLIC PERFORMANCE 227 (James E. Katz & Mark A. Aakhus eds., 2002) (exploring “absent presence,” especially in relation to communication technology).

271. See generally JAMES E. KATZ, *MAGIC IN THE AIR: MOBILE COMMUNICATION AND THE TRANSFORMATION OF SOCIAL LIFE* (2006) (examining effects of mobile and pervasive communications technology on daily interaction).

272. Cass Sunstein has referred to the private filtering or narrowcasting of information as the “Daily Me,” a technological bubble that channels pre-selected content to the listener or viewer. See CASS R. SUNSTEIN, *REPUBLIC.COM* 7 (2001) [hereinafter SUNSTEIN, *REPUBLIC.COM*].

273. See generally SUNSTEIN, *DISSENT*, *supra* note 145, at 1-13 (describing how groups make better decisions when dissent and debate are present).

274. See STEVEN FLUSTY, *BUILDING PARANOIA: THE PROLIFERATION OF INTERDICTIONARY SPACE AND THE EROSION OF SPATIAL JUSTICE* 12 (1994) (noting importance of chance encounters to civic life).

275. See MICHAEL BULL, *SOUND MOVES: IPOD CULTURE AND URBAN EXPERIENCE* (2006) (examining how the iPod and other portable devices are changing the audio experience of public places).

276. See Frug, *supra* note 263, at 1092 (describing new urbanist efforts to make public space

more user-friendly places. But the quality of public presence and interaction, particularly as it concerns the exercise of public expressive liberties, is another matter. If we turn our public places into home offices and shield ourselves in mobile technology bubbles, people will become increasingly disconnected in public. The phenomenon of absent presence will negatively affect the identity, participation, and transparency functions of public places.

3. The Purification of Public Places

Chance encounters and expressive noise will not be the only things missing in networked public places. Other forms of spatial purification will also occur. Again, public places serve their functions best when a multitude of expressive forms—symbols, acts, and theater—are present. As noted, urban social critics contend that the modern built environment places a premium on recreation and mass consumption rather than social interaction.²⁷⁷ The networking of public places will exacerbate this problem in ways that we are only now beginning to appreciate.

Urban geographers have offered a very strong case to the effect that public surveillance, in particular, will cause a purification of public places. Open and dynamic places will be “replaced by pseudo-public spaces like those in shopping malls, where commercial imperatives dominate and what goes on, and who participates, is intensely regulated and tightly controlled so that profitable consumption is maximized.”²⁷⁸ As these places facilitate more and more consumption, they will leave less and less space for ordinary expressive activities.

Even in once quintessential public places, protest and dissent in particular may be deemed almost entirely out of place, because of the gaze of constant surveillance. Professors Kang and Cuff show rather convincingly how embedded computing in malls—their chosen spatial paradigm—can “control access, facilitate policing, [and] minimize loitering.”²⁷⁹ These effects are not, of course, limited to malls. The combination of surveillance, digital awareness, and constant identification may just as readily be used to control access to and facilitate policing of parks, squares and other public places.

If applied across the full range of the expressive topography—from

more interactive).

277. See Michael Sorkin, *Introduction to VARIATIONS ON A THEME PARK*, *supra* note 243, at XI (describing cities as theme parks revolving around consumption while sacrificing human interaction); FLUSTY, *supra* note 274, at 12.

278. Michael McCahill, *Beyond Foucault: Towards a Contemporary Theory of Surveillance*, in *SURVEILLANCE, CLOSED CIRCUIT TELEVISION AND SOCIAL CONTROL* 41, 52 (Clive Norris, Jade Moran & Gary Armstrong eds., 1998).

279. Kang & Cuff, *supra* note 4, at 121.

malls to parks to squares—network controls may substantially affect the identity, self-governance, and transparency functions of public places. For instance, Kang and Cuff note that in a mall, technology could provide “an additional, more sophisticated and granular layer of access control.”²⁸⁰ Individuals might be discouraged from entering the space of the mall by means of a “blacklist” generated by a combination of computer algorithms and embedded tags and devices.²⁸¹ If patron identification difficulties could be resolved, perhaps by some sort of frequent-shopper tag or card, Kang and Cuff note the possibility of exclusion of “those with any brush with law enforcement, mental illness, or civil disturbance could be seen as socially reasonable.”²⁸²

Public places like squares and parks might be similarly purified of potential threats to public order and safety. Using the full network power of video surveillance, future biometric technologies, wireless Internet data, and mobile GPS devices, it may be possible to identify in advance and exclude certain persons from demonstrations, campaign events, or other public gatherings. The policing of place, which would be mostly covert, might even be used to detain or discourage certain speakers. This is not the stuff of science fiction fantasy. At least one company claims to have developed “a fully automated facial recognition system based on neural network software . . . which can scan the faces of the crowd in ‘real’ time and compare the faces with images of known ‘troublemakers’ held on a digital database.”²⁸³ In an era when preemptive governmental intervention and watch lists are increasingly becoming the norm, it is not hard to imagine officials seeking to prevent potentially disruptive protesters from occupying certain public places in advance.

The networking of public places may, however, have even broader effects on the identity and participation functions. Evidence from social science suggests that women, the homeless, and people of color experience being in *material* public places differently than do other citizens.²⁸⁴ Scholars have noted that public surveillance “raises major questions about geographic change, social control, patterns of inclusion and exclusion . . . and the spatial dynamics of the so-called information society.”²⁸⁵ Some studies also indicate that officials use surveillance technologies to purify

280. *Id.* at 122.

281. *Id.*

282. *Id.* at 124.

283. NORRIS & ARMSTRONG, *supra* note 166, at 217.

284. See NIELSEN, *supra* note 148, at 6 (noting that “simply being in public is different for white women, people of color, and those in poverty”).

285. Stephen Graham, *Spaces of Surveillant Simulation: New Technologies, Digital Representations, and Material Geographies*, in 16 ENVIRONMENT AND PLANNING D: SOCIETY AND SPACE 483-504 (1998).

public places of groups like the homeless and teenagers.²⁸⁶ Others have shown that surveillance has targeted women for voyeuristic reasons and has been used to profile racial minorities.²⁸⁷ Other groups, including homosexuals, may also experience networked public places differently.²⁸⁸ Today, of course, it is not difficult to imagine Muslim citizens living a chilled public life in places where every word and gesture is potentially subject to official and unofficial surveillance techniques.²⁸⁹

Surveillance is not the only network feature that may chill certain forms of expression and association. Professors Kang and Cuff ask:

How likely are you to walk through the gay and lesbian studies section of Borders if you are closeted and know that RFID readers are locked on your body? How likely will you be to grouse about the administration if you are an Arab American male, walking with fellow Arab American friends, after the Department of Homeland Security has just warned about terrorist plots in the malls?²⁹⁰

Eventually, embedded technologies like digital tags will raise these sorts of concerns in *all* public places. A constantly authenticating spatial environment may drive certain forms of identity and participation underground—or at least away from certain networked public places.²⁹¹ While some may be encouraged by features like wireless access to populate networked places, others may be deterred from doing so by other features of the networked environment.

The upshot is that in presently very difficult to quantify ways, the networking of public places may have a leveling and sterilizing effect on public expressive life. Certain individual and group speech activities may be less and less visible in networked places. Certain forms of speech may begin to disappear as the phenomenon of anticipatory conformity cleanses

286. Katherine S. Williams & Craig Johnstone, *The Politics of the Selective Gaze: Closed Circuit Television and the Policing of Public Space*, 34 CRIME, L. & SOC. CHANGE 183, 193 (2000).

287. See Koskela, *supra* note 146, at 257-78; Williams & Johnstone, *supra* note 286, at 193.

288. See Jeffrey Rosen, *A Watchful State*, N.Y. TIMES, Oct. 7, 2001, § 6 (Magazine), at 38, 93 (noting homosexuals may be inhibited by the presence of public surveillance cameras).

289. See Andrea Elliott, *After 9/11, Arab Americans Fear Police Acts, Study Finds*, N.Y. TIMES, June 12, 2006, at A15; see also Blitz, *supra* note 6, at 680-81 (examining implications of monitoring urban spaces in order to protect against terrorist threats).

290. See Kang & Cuff, *supra* note 4, at 127 (footnote omitted); see also Cohen, *supra* note 4, at 31 (noting that “the shift to networked space changes the character of existing space even for those people who are unaware of its presence”).

291. See Clive Norris, *From Personal to Digital: CCTV, the Panopticon, and the Technological Mediation of Suspicion and Social Control*, in SURVEILLANCE AS SOCIAL SORTING: PRIVACY, RISK AND DIGITAL DISCRIMINATION 278 (David Lyon ed., 2002) (noting that “it is the computer—not the camera—that heralds the panopticonization of urban space”).

public places of all but the most acceptable displays.²⁹² Dissent and disruption, which are already subject to a growing number of material spatial regulations, will be even less likely to appear in networked public places.²⁹³ Privacy experts have noted that surveillance and data retention tend to substantially dampen spontaneous behavior.²⁹⁴ These things internalize control and produce a degree of self-vigilance.²⁹⁵ Whether or not any of these effects is sufficient to constitute the prohibited chilling of expression, they will most certainly affect the expressive functioning of public places.

Many of the features of networked public places will operate in a non-transparent, even covert, fashion. They will have the effects noted above in part because people will not know to what extent they are being watched, by whom, or for what purpose.²⁹⁶ The automated nature of some new surveillance methods,²⁹⁷ the anonymity of methods of control and regulation, and a general uncertainty about the scope and use of the public record may breed further mistrust of government, resentment of public officials, and consequent avoidance of public places.

The networking of public places will further diminish what one geographer has called the "democratic admixture on the pavements."²⁹⁸ It may ultimately contribute to what another scholar calls "the current urban malaise."²⁹⁹ In the purified public square, identity claims and

292. See *supra* note 168 and accompanying text; see also Philip Tabor, *I Am a Videocam*, in *THE UNKNOWN CITY: CONTESTING ARCHITECTURE AND SOCIAL SPACE* 122, 135 (Iain Borden et al. eds., 2001) ("The very idea of surveillance evokes curiosity, desire, aggression, guilt, and, above all, fear—emotions that interact in daydream dramas of seeing and being seen, concealment and self-exposure, attack and defense, seduction and enticement.").

293. For a discussion of spatial controls, see generally Zick, *Speech and Spatial Tactics*, *supra* note 7 (noting that public spaces are increasingly controlled by spatial regulations that increase social and political control).

294. See Slobogin, *supra* note 5, at 243-44; see also Richard Wasserstrom, *Privacy: Some Arguments and Assumptions*, in *PHILOSOPHICAL DIMENSIONS OF PRIVACY* 325-26 (Ferdinand David Schoeman ed., 1984).

295. Hille Koskela, 'The Gaze Without Eyes': Video-Surveillance and the Changing Nature of Urban Space, 24 *PROGRESS IN HUMAN GEOGRAPHY* 243, 253 (2000).

296. Urban geographers and criminologists have compared the effect of network surveillance to the concept of Jeremy Bentham's Panopticon, a structure that leverages the power of spatiality and surveillance to keep prisoners guessing as to whether, when, and how their actions were being monitored. See, e.g., DAVID LYON, *SURVEILLANCE SOCIETY: MONITORING EVERYDAY LIFE* 108 (2001); see also MICHEL FOUCAULT, *DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON* 195-228 (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1977) (discussing the Panopticon).

297. See Gary T. Marx, *What's New About the "New Surveillance"?: Classifying for Change and Continuity*, 1 *SURVEILLANCE AND SOC'Y* 8, 28-29 (2002), available at <http://www.surveillance-and-society.org/articles1/whatsnew.pdf> (noting automation of new surveillance technologies).

298. MIKE DAVIS, *CITY OF QUARTZ: EXCAVATING THE FUTURE IN LOS ANGELES* 231 (1990).

299. Jon Bannister, Nicholas R. Fyfe & Ade Kearns, *Closed Circuit Television and the City*, in *SURVEILLANCE, CLOSED CIRCUIT TELEVISION AND SOCIAL CONTROL*, *supra* note 278, at 21-22.

unconventional modes of participation will be segregated and managed by non-transparent networking features like surveillance and automated identification.³⁰⁰ Public places will be far less attractive venues for self-governance and other public democratic functions.

D. *Retaining the Civic Character of Public Places—Some Modest Proposals*

The networking of public places may challenge the democratic and expressive functioning of places by creating a new public digital divide, distracting public speakers and audiences, and further sanitizing public venues. It is important to recognize these potential effects in advance of the full networking of public places. There is no preventing this networking. It will happen. Indeed it is already happening. But there are some steps that might be taken to counteract at least some of these changes, thus preserving or at least making possible more robust civic and expressive public places. This section briefly discusses a few modest proposals that relate to preserving the basic First Amendment functions of public places.

1. Ownership and Access

As access to communications technologies becomes increasingly critical to the identity and participation functions of networked public places, *differential* access to these technologies necessarily becomes a greater concern. The focus in studies of the digital divide has thus far been on access provided in private places like the home or public settings like schools.³⁰¹ Given the strong trend toward public place networking, we must now also begin to address a nascent divide that will affect *public* expressive space on a large scale.

In the not-so-distant future, access to the latest technologies of communication will be required for effective communication—with government in some cases and with fellow citizens in others—in public places. Thus the manner in which municipalities provide public Web access will be critically important to public expression. To maintain the leveling quality of public places, it will be increasingly important that as many citizens as possible have access to the latest technologies.

It is important that municipalities that provide wireless public access own and maintain their networks. Like roads, wireless networks will

300. See Don Mitchell, *The End of Public Space? People's Park, Definitions of the Public, and Democracy*, 85 ANNALS OF THE ASS'N OF AM. GEOGRAPHERS 108, 115 (1995) (noting that surveillance creates "planned, controlled, ordered space") (footnote omitted).

301. See, e.g., U. S. DEPT. OF COMMERCE, *supra* note 266 (measuring access to the Internet in homes and schools).

require continuous upgrades. Individual companies or groups of service providers may not be willing to undertake the necessary repairs. In addition, by owning the networks officials can ensure that the public has open access to them. Like the streets themselves, wireless clouds should not be subject to myriad private access restrictions. If cities are committed to providing this new means of communication, they should be willing to invest substantially in the expressive infrastructure of the future.

In addition, the provision of tiered public access is particularly troublesome. The desire to subsidize public costs is understandable. Public Internet access ought, however, to be *freely* available to members of the public. There should not be *classes* of wireless connectivity, with the highest speeds and applications available only to those with the means to pay. This would be like restricting some citizens to a virtual sidewalk while others speed past on a *moving* sidewalk. There are, of course, circumstances in which citizens are required to pay for access to the means of communication. For example, permitting schemes for demonstrations and parades sometimes require pre-insurance or the posting of a bond.³⁰² But these requirements generally relate to possible damage that might result from the expressive activity. The public Web platform—the clouds and meshes above public areas—is not characterized by scarcity or any other cost resulting from specific or additional users. Thus, there ought to be no permit fee for public wireless use.

Access concerns extend beyond wireless portals. In the fully networked environment a mere Internet connection will not suffice to facilitate effective expression. Public citizens will need the appropriate mobile technologies as well. These mobile devices will link people to the public network. Hand-held, worn, and portable communications technologies will become basic requisites for communicating with institutions and governments. Public safety announcements, for example, may be delivered over public networks. Devices will also be needed for social networking and collective public action. As Kang and Cuff suggest, a “datasense” will be required for full participation in public life. Governments of course have no constitutional obligation to subsidize access to the latest communications technologies. But if they are going to facilitate public connectivity then they should also consider supporting access to the communicative technologies needed to communicate in a networked environment.³⁰³

302. See C. Edwin Baker, *Unreasoned Reasonableness: Mandatory Parade Permits and Time, Place, and Manner Regulations*, 78 NW. U. L. REV. 937, 992 (1983) (analyzing parade permit requirements).

303. See SUNSTEIN, REPUBLIC.COM, *supra* note 272, at 182-89 (addressing means for facilitating access to diverse viewpoints, including redesign of web pages and government subsidies).

2. Regulatory Transparency

As noted, surveillance may substantially affect use of networked public places. Citizens' knowledge of official access and other controls in public places may turn out to be critical to the functioning of public places and public expression.

As others have advised, governments should start now to develop protocols and regulations that limit public surveillance activity and the collection and retention of citizen data.³⁰⁴ Adoption of surveillance programs should be the result of an open and transparent public process. Among other things, communities should seriously and publicly debate whether they need a surveillance system at all. Installation should be based not on whether federal or state funds are available but a fair assessment of whether public surveillance of an area is actually needed to address a real safety or security concern. Any surveillance program should be closely tailored to the publicly stated governmental purpose supporting it. This tailoring should include treatment of the degree of surveillance sophistication needed to serve official purposes. Biometrics and other invasive technologies should rarely, if ever, be used to monitor public places.

Permanent surveillance of the sort currently operated by the National Park Service also should not be used in public places.³⁰⁵ Its use is fundamentally inconsistent with the history, tradition, and functions of places like the National Mall. Even in the ordinary public square, always- or usually-on surveillance cameras should not be implemented absent a clear and publicly justified safety concern. Again, there must be public input as to any proposed surveillance. Public debate regarding any such programs should include serious consideration of their effects on public liberties like expression and association.³⁰⁶

As importantly, citizens should have assurances that the public data trails they leave behind are not being collected, stored, mined, or used for improper purposes. This observation applies to Muni WiFi programs and surveillance camera programs alike. It is not enough that municipalities assure that they will not mine private data. Officials must consider protocols and regulations for the storage, retention, and retrieval of public WiFi data. With respect to both Muni WiFi and public surveillance programs, officials should create technological and administrative

304. See Slobogin, *supra* note 5, at 286-312 (proposing adoption of measures to implement right to public anonymity). For a comprehensive list of suggestions for public surveillance programs, see THE CONSTITUTION PROJECT, *supra* note 78, at 15-25.

305. THE CONSTITUTION PROJECT, *supra* note 78, at 16.

306. *Id.* at 18-19 (discussing constitutional concerns and "social 'costs'" of surveillance).

safeguards that will encrypt publicly transmitted data, limit access to that data, and provide clear guidelines for non-law enforcement access to surveillance records.³⁰⁷ Once again, adoption of these protocols and regulations should be the result of an open public process.

Public transparency and accountability will not ensure that expressive and associate chill or the sanitizing of public places will not occur. But these are minimal steps that can and should be taken to assure citizens that public places remain open to identity claims and participatory self-governance.³⁰⁸ It is unfortunate that surprisingly few governments have taken any of these steps to date.³⁰⁹ The National Park Service, for example, has neither sought public input with respect to its surveillance practices on the National Mall and other critical public properties nor disclosed the nature or extent of that surveillance program to the public.³¹⁰ It is precisely this sort of lack of transparency that may lead to avoidance and purification of public places.

3. Protest Tactics, “Sousveillance,” and Civil Disobedience

Even with these safeguards, we will sometimes be watched when we are in public. We cannot rely solely on governments to provide transparency. Public places are ultimately a matter of public responsibility. Just as civil rights protesters experimented with the sit-in and other expressive actions in response to official controls, so too must the modern citizen think and act more creatively to preserve spaces for public expressive activity.

As mentioned earlier, technological advances associated with the networking of public places might be used to the advantage of public protesters and demonstrators.³¹¹ With always-on public wireless networks and personal computing devices, speakers and assemblies can engage in swarming and other tactical maneuvers that will render public displays more effective.³¹² The power of computer-enhanced social networking can be used to counteract some of the most severe official regulations on public assembly and expression, including material space restrictions on movement and spontaneity. Speakers will be able to communicate with one another over vast public spaces, in real time. Official tactics for controlling public protests and demonstrations, including corralling and zoning public speakers, might be thwarted or at least challenged by

307. *Id.* at 20 (encouraging adoption of surveillance protocols and controls).

308. *Id.* at 25-35 (providing additional guidelines for the use of public surveillance systems).

309. *Id.* at 10-13.

310. *See supra* note 80 and accompanying text.

311. *See supra* notes 86-89 and accompanying text.

312. *See RHEINGOLD, supra* note 87, at 157-58 (discussing instances in which “smart mobs” used technology to thwart official efforts to regulate public displays).

counter-tactics like “snake marches” and other spontaneous counter-movements.³¹³

Smarter protests are not the only advance that may limit the repressive effects of spatial networking. As mentioned, an army of citizen-journalists will occupy networked public places. Their cameras will create an unofficial record of what occurred before, during, and after public expressive events. On the pragmatic front, this may serve as crucial evidence when protesters seek to defend themselves from charges of breaching the peace, disorderly conduct, or resisting arrest.³¹⁴ More generally, however, it may restore public confidence in the ability to act out and up in public without fearing that an official record of events will be the only record available in subsequent proceedings. Private surveillance will contribute to public regulatory transparency, as the police and other officials are themselves constrained by surveillance.

Recording events and publishing them to the Web in real space and time will also permit protesters to bypass media filters that tend to distort protest messages. Citizen-journalists can create and publish a Web page as events unfold. Members of an assembly can determine the content of these presentations as well as their focus as published.

The use of cameras at protests is merely one form of “sousveillance,” or surveillance *from below*.³¹⁵ Electrical engineers and sociologists are currently partnering to design wearable computers that in effect watch our official watchers.³¹⁶ This inverse or counter-surveillance re-situates the technologies of surveillance, essentially turning the tables on authorities. Sousveillance does not eliminate public surveillance. But it may encourage people to engage and dispute rather than fear and thus avoid public surveillance—and public places. It signals to authorities that citizens are aware of but not intimidated by the presence of surveillance devices. In this sense sousveillance can be an empowering activity.

313. Snake marches are responses to permitting schemes that seek to control the location and movement of public demonstrations. Rather than apply for a permit, protesters “snake” in and out of streets and roadways. See Luis Fernandez, *Policing Space: Social Control and the Anti-Corporate Globalization Movement*, CANADIAN J. OF POLICE & SECURITY SERVS., Winter 2005, at 247.

314. See Jim Dwyer, *Videos Challenge Hundreds of Convention Arrests*, N.Y. TIMES, Apr. 12, 2005, at A1 (reporting how a “sprawling body of visual evidence, made possible by inexpensive, lightweight cameras in the hands of private citizens, volunteer observers and the police themselves” was used by protesters to defend against charges).

315. See Steve Mann, Jason Nolan & Barry Wellman, *Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments*, 1 SURVEILLANCE & SOC’Y 331, 332 (2003), available at [http://www.surveillance-and-society.org/articles1\(3\)/sousveillance.pdf](http://www.surveillance-and-society.org/articles1(3)/sousveillance.pdf) (describing experiments with sousveillance devices).

316. *Id.* at 338-46; see also DAVID BRIN, *THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM?* 159-60 (1998) (discussing various counter-surveillance technologies).

In addition to engaging in their own forms of counter-surveillance, citizens can also resist technologies through non-compliance and even, in some cases, active interference with cameras.³¹⁷ They can, for example, force governmental transparency by sharing information on the Web about the location of surveillance cameras. A creative group known as the Surveillance Camera Players uses a form of street theater to highlight and expose the location and operation of cameras in New York City.³¹⁸ This very mild form of civil disobedience actually uses a combination of public speech, assembly, and network technology to impose transparency on public surveillance programs.

New restrictions on public expression call for new tactics of resistance. Counter-surveillance and public awareness campaigns can be effective in drawing attention to and imposing transparency on public surveillance systems. This may provide some assurance and confidence to public protesters otherwise concerned about the repressive effects of networked public places.

4. Laws, Norms, and Architectures

How the networking of public places affects public expressive behavior will ultimately depend upon some combination of laws, social norms, and architectures.³¹⁹ Of course, legislators could pass new laws to deal with things like drive-by pornography, public spamming, and new forms of cyber-stalking. Citizens might adjust their behaviors to take the effects of new technologies on public life into account. Engineers could create products that facilitate selective receipt of speech and permit surveillance without destroying public liberties.

If there is one clear lesson from the analysis of networked places in this Article it is that laws will be increasingly ineffective in terms of regulating public expression. In many cases networked expression will be too slippery to be regulated and too disconnected from material places to be effectively policed. Enacting new laws will not preserve the democratic functions of public places. Norms and architectures will be far more effective than laws in terms of protecting us from harmful public speech and preserving public anonymity.³²⁰

317. See Gary T. Marx, *A Tack in the Shoe: Neutralizing and Resisting the New Surveillance*, 59 J. OF SOC. ISSUES 369, 374-84 (2003) (discussing a host of tactics people can use to neutralize and resist efforts to collect personal information).

318. The players are described on their website, The Surveillance Camera Players: Completely Distrustful of All Government, <http://www.notbored.org/the-scp.html> (last visited Nov. 13, 2006).

319. See LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 19-22 (1999) (noting that law, social norms, architecture, and the market regulate social behavior).

320. See Blitz, *supra* note 6, at 718 (noting that preserving expressive liberties in public spaces is often "a question of architectural design and planning rather than of First Amendment law");

We will all have to learn to live with the thrusting of expression we find offensive and distasteful. This will require honing our ability to selectively consume information. It will require some community policing of public places—parents shielding children from sexually explicit information, and public shaming of “dirty drivers” and consumers of pornography in public parks and on public subways, trains, and buses.³²¹ Like the traditional press, citizen-journalists armed with cameras and recorders will have to exercise restraint in training their devices on private actors in public places. We will all have to become more mindful that in casting our eyes downward and plugging our ears, we are destroying aspects of the public expressive culture.

Most important, perhaps, will be the architectures of computer codes for the devices we wear and carry and the environment we will inhabit. The key will be to design codes that will simultaneously facilitate the open exchange of information and monitor space in a fashion that preserves that same openness. Software engineers and the architectures they construct will be far more important to networked expressive culture than legislative or executive decrees.³²² These systems will establish protocols of protection from unwanted or harassing public expression delivered from mobile devices. They will permit us to authenticate our identity or mask it.

Governments are responsible for taking expressive liberties into account as they commission new systems and digitize the public environment. Of course, we are all responsible for using products and programs in a manner that preserves public expressive liberties. As compelling as our own sound tracks may be, we must recognize that we miss much by heavily filtering our public experiences.

None of these rather modest proposals will guarantee a return to public places or a robust public expressive culture there. But as public places become networked, we must begin to consider how we might preserve what remains of the identity, self-governance, and transparency functions of public places.

V. CONCLUSION

We have arrived at a critical period of transition insofar as public places and public expression are concerned. The material places we have

Werbach, *supra* note 101 (also emphasizing the importance of social norms).

321. See LEE C. BOLLINGER, *THE TOLERANT SOCIETY: FREEDOM OF SPEECH AND EXTREMIST SPEECH IN AMERICA* 12 (1986) (noting that social controls like ridicule, humiliation, and social shunning are often effectively used to regulate offensive expression).

322. See Kang & Cuff, *supra* note 4, at 136-39 (proposing various design features to make surveillance at malls more transparent).

traditionally occupied—and which have substantially influenced norms, expectations, and legal doctrines relating to public expression—are becoming highly networked. As a result, traditional distinctions between private and public speech, and online and offline presence, are rapidly fading into extinction.

The First Amendment implications of the progression toward networked public places are serious. Much depends on the scope and use of technological advances. Already, however, we can be relatively certain that public citizens will become more captive to certain forms of unwanted expression, more known (or at least knowable) to governmental authorities as they gather and speak in public, and less and less personally engaged in expressive communion with one another in public places. There are pressing questions with regard to whether, and if so how, old First Amendment doctrines and principles might be transported into modernized places.

Of even larger concern are the prospects for continued self-governance through and in public places. Reducing the spaces of offline presence by providing public wireless networks may replenish public places to some degree. But the people there will be less connected as a result of the pervasive personal computing they will bring with them. The squares and parks they will occupy will likely be even more purified and sterile than the commercialized malls many public places have already become. Certain marginalized groups and activities may be even less welcome in networked public places than they have been in traditional material ones.

We cannot reverse the progression toward networked public places. The forces trending in this direction are much too strong. The features of public place networking that are most threatening to public expression can, however, be managed. If the public square is to be networked, then governments must concentrate on expanding access to crucial means of public communication, both in terms of wireless access and the tools that ensure public connectivity. Citizens must press officials to make the networking of public places a more transparent and politically legitimate process. They must also learn to use new technologies to enhance their own expressive liberties. Public citizens must use communication devices responsibly such that they do not infringe on the public liberties of others. In networked public places, formal laws and constitutional principles will matter less to the scope of expressive liberties than will new computer codes and the behavioral norms that shape their applications.