UCLA
Papers

Title
Pervasive Computing: Embedding the Public Sphere

Permalink
https://escholarship.org/uc/item/0qt608kr

Authors
Kang, Jerry
Cuff, Dana

Publication Date
2005-05-20

eScholarship.org Powered by the California Digital Library
University of California

Pervasive Computing: Embedding the Public Sphere

Jerry Kang*
Dana Cuff**

Table of Contents

---

* Visiting Professor of Law, Harvard Law School 2003–04. Visiting Professor of Law, Georgetown University Law Center 2004–05. Professor of Law, UCLA School of Law. Contact: kang@law.ucla.edu, http://jerrykang.net

** Professor, UCLA Department of Architecture and Urban Design. Contact: dcuff@ucla.edu. This project emerged from our co-directing the Institute of Pervasive Computing and Society (iPerCS), funded by UCLA's Chancellor Albert Carnesale. The UCLA Academic Senate, the UCLA Asian American Studies Center, the UCLA School of Law, and the Harvard Law School also contributed funds to support this Article. Eddy Johnson and the Hugh & Hazel Law Library at UCLA provided able research assistance. We thank readers of earlier drafts: David Barron, Yochai Benkler, Julie Cohen, Deborah Estrin, Terry Fisher, Ken Fishkin, Charles Nesson, Adam Neufeld, Greg Pottie, Pam Sammelson, Joseph Singer, Marc Smith, Eugene Volokh, Jonathan Weinberg, Norton Wise, and Jonathan Zittrain.

I. Introduction

Pervasive Computing (PerC) is what happens when the Internet gets ubiquitous, embedded, and animated. Ubiquitous access to the Internet through mobile, wireless devices is imminent. More important and less understood, the Internet will soon invade real space as networked computing elements become embedded into physical objects and environments. Through this implantation, the physical world will gain digital qualities, such as computer-addressability through unique identification codes. Because these elements can also be animated, the environment will be able to respond directly to what it senses.

Like digital kudzu, PerC will spread and cyberize what we have tenuously preserved as "real space." If the line between cyberspace and real space has grown increasingly difficult to draw, it may soon become impossible.[1] Widespread implementation of PerC will mean that the Internet will always be around—in the air and the walls—providing an ever-ready information template overlaid on the "real" world we navigate.[2] In addition, by embedding computing into the physical world, PerC will bring the qualities of cyberspace, including some of its information economics, into the material

1. The standard distinction in cyber-literature now is between "real" space (that which has physical properties) and the "virtual" (having no physical properties). Pervasive computing's "embodied virtuality" erodes that distinction. *See* Mark Weiser, *The Computer for the 21st Century*, SCI. AM., Sept. 1991, at 94, 94–95 (noting that "embodied virtuality" refers "to the process of drawing computers out of their electronic shells" and bringing virtual information into the physical world).

2. Driving with the assistance of real-time global positioning systems (GPS) provides one sense of what such an overlay might feel like. *See* Alex L. Goldfayn, *GPS Finds a Place in Cars*, CHI. TRIB., June 7, 2003, at C4 (describing a GPS system telling the driver when to turn in real time), *available at* 2003 WL 56161454.

realm. It will enable the cyberized environment to respond, perhaps autonomously, to data previously uncollected and uncollectible. Imagine not a robot, not an isolated and identifiable device, but a world saturated with networked intelligence.

We can speculate about benefits, such as increased personal safety by better monitoring of public spaces. Just as easily, we can speculate about costs, such as diminished privacy through excessive surveillance. Will these benefits and costs, as well as other political, social, and ethical concerns, be adequately vetted before PerC becomes a pervasive reality? We doubt it, especially given PerC's decentralized research and development, piecemeal adoption, obvious cost savings, and deep invisibility.

This Article is a necessarily transdisciplinary intervention[3] into how PerC becomes embedded into our public sphere, in the sense of public spaces, and conversely how the public sphere, in the sense of the cultural, ethical, and policy judgments made through public discourse, might be embedded into PerC itself. We seek to spot major issues, provide an analytic vocabulary, and initiate preliminary analyses. Predicting, much less advising about, even near-futures may be in vain. Still, given what is at stake, we take up that challenge.

II. Pervasive Computing

A. PerC Defined

The term "pervasive computing" does not have any orthodox definition. We use this term to describe the kind of computing that will result from the convergence of three computing-communication trends.

Ubiquitous. Access to information—best represented by current use of the Internet—will become ubiquitous. Right now, most people use the Internet while sitting in front of desktops with a wired network connection. But that model of data access is changing rapidly. First, the nodes used to access the Internet are diversifying and shrinking. In addition to notebook computers and tablet PCs, personal digital assistants (PDAs) as well as mobile telephones are increasingly providing limited, but useful, access to the Internet. Indeed, previously separate electronic devices are converging into communicators that

3. To our knowledge, this is the first law review article coauthored by academics from the fields of law and architecture. (We thank our colleague Greg Pottie, Engineering, for his insights on technical matters.) For a thoughtful examination of architecture within the law reviews, see generally Neil Kumar Katyal, *Architecture as Crime Control*, 111 YALE L.J. 1039 (2002).

provide not only voice telephony but also access to the World Wide Web, email, instant messaging, and other communicative functionalities in a single, compact form-factor.[4] Second, the channel of communications is increasingly becoming wireless and widespread in the form of 802.11x wireless local area networks (Wi-Fi), 3G (third generation) mobile telephony networks, and even newer technologies.[5]

Access nodes will further shrink in size and grow in power, with correlative improvements in user interfaces to make the information received legible (for example, with visor interfaces, or anywhere-readable communicator screens) or otherwise comprehensible (for example, with spoken messages through wireless ear prosthetics).[6] In the next two decades, we expect tremendous advances in both coverage and bandwidth of wireless channels, especially in urban environments. The Internet will soon become accessible in nearly all nonrural places, through technologically facile, culturally accepted, and highly functional devices.[7]

---

4. New mobile telephone plus personal digital assistant combinations appear almost monthly. Popular variations include models produced by Research in Motion (Blackberry), palmOne (Treo), and Danger (hiptop, also known as sidekick). Other communicative functionalities that are being added include video streaming, television, photography, video recording, video gaming, and geolocation.

5. *See* Yochai Benkler, *Some Economics of Wireless Communications*, 16 HARV. J.L. & TECH. 25, 36–47 (2002) (describing a possible wireless infrastructure that relies on "smart" receiving devices that can decode and retransmit signals). Such a system could eliminate the need to assign specific frequencies to specific carriers in order to avoid interference. Instead, similar to the current Internet, smart devices could listen to the entire spectrum and pick out only the relevant packets of information. *See id.* at 42 (describing computer receivers that can listen to a "very broad range of frequencies, and instead of differentiation between sources of radiation by their relative power they identify radiation patterns that coincide with the code that they know is associated with the transmission they are listening for"). Moreover, capacity could scale with demand because each new user's device could also help transmit data along. *See id.* at 44–46 (describing a network where new "users add capacity at least proportionately to their added demand"). In this way, each new receiver also acts like a new transmitter. For a skeptical review of the technology and its legal implications, see generally Stuart Minor Benjamin, *Spectrum Abundance and the Choice Between Private and Public Control*, 78 N.Y.U. L. REV. 2007 (2003).

6. Other visual interfaces could include "display motes," which are wristwatch-sized displays scattered around environments that can display information. We often look for a clock in the room to see what time it is. In the future, we might look around for a mote to read some accessible data.

7. We are mindful of the digital divide that persists. *See generally* HIGH TECHNOLOGY AND LOW-INCOME COMMUNITIES: PROSPECTS FOR THE POSITIVE USE OF ADVANCED INFORMATION TECHNOLOGY (Donald A. Schön et al. eds., 1999). Internet penetration on Native American reservations, for example, is likely low. The most recent study by the National Telecommunications and Information Administration did not include figures for American Indians. ECONS. & STATISTICS ADMIN., NAT'L TELECOMMS. & INFO. ADMIN., U.S. DEP'T OF

Embedded. In addition to ubiquity, we use the term "PerC" to capture computing's melding into the physical world. As the Y2K bug fears demonstrated, computers are not only on our desktops; they are already everywhere—in our appliances, our buildings, our automobiles, our basic infrastructure. Imagine the further miniaturization and improvement of these computing elements, both in terms of processing and communication,[8] consistent with Moore's Law.[9] These computing elements can be embedded within physical devices like watches or the environment itself, as in walls. They can be molded into furniture, stitched into clothing, printed on food packaging, and could someday become small and resilient enough to mix into house paint or spray over a toxic spill. Capable of wireless communications, these devices may even be smart enough to self-organize into localized networks.

One prominent PerC technology that ushers in the future is the embedded radio frequency identification (RFID) tag. These miniature tags emit a unique identification number that can be read from a distance by an RFID reader. Passive RFID tags lack an energy source and instead use the initial signal from the reader to power their transmission back to the reader. These readers may

---

COMMERCE, A NATION ONLINE: HOW AMERICANS ARE EXPANDING THEIR USE OF THE INTERNET 21 n.10 (2002), *available at* http://www.ntia.doc.gov/ntiahome/dn/anationonline2.pdf (on file with the Washington and Lee Law Review). Yet telephone penetration is only 67.9% among Indians on reservations or off-reservation trust lands, compared to the national average of 95%. INDUS. ANALYSIS & TECH. DIV., FCC, TELEPHONE SUBSCRIBERSHIP ON AMERICAN INDIAN RESERVATIONS AND OFF-RESERVATION TRUST LANDS 1 (2003), *available at* ftp://www.fcc.gov/pub/Bureaus/Common_Carrier/Reports/FCC-State_ Link/IAD/subsai03.pdf (on file with the Washington and Lee Law Review).

8. The same silicon technologies that exponentially improve processing speed also improve communications, in both signal processing and radio frequency circuits. *See* COMM. ON NETWORKED SYS. OF EMBEDDED COMPUTERS, NAT'L RESEARCH COUNCIL, EMBEDDED, EVERYWHERE: A RESEARCH AGENDA FOR NETWORKED SYSTEMS OF EMBEDDED COMPUTERS 49 (2001) [hereinafter EMBEDDED EVERYWHERE] (noting that the scaling of these silicon technologies "enables cheap signal processing and low-cost radio frequency circuits" that drive down the cost of communication for both wireline and wireless systems).

9. Moore's Law states that computer processing capability doubles approximately every eighteen months. *See* HARRY NEWTON, NEWTON'S TELECOM DICTIONARY 573 (16th and a half ed., 2000) (noting that Intel Corporation co-founder Gordon Moore has forecasted that computer chip complexity will double every eighteen months for the next decade). Moore's Law is not a law of physics akin to the Second Law of Thermodynamics; rather, it is an observation about the improvement of silicon technologies over time. Our engineering colleague Greg Pottie suggests that Moore's Law should be understood as mostly an economic "law" because it has applied even before silicon became the material basis of computing. He suggests that there is essentially an insatiable demand for computing so the resources necessary are poured into increasing computing power; however, at least eighteen months are necessary for investors to recover their capital investment.

soon be able to operate economically at a distance of five to fifteen feet, without clear line-of-sight to the RFID tag. Active RFID tags, which utilize some power source,[10] could have longer ranges. As these tags get smaller and cheaper to produce, they will replace universal bar codes.[11] Installed initially for inventory management by manufacturers and distributors,[12] these embedded tags will be everywhere.[13]

Animated. Now, add to these miniature computing-communication devices the functionality provided by recent advances in microelectricalmechanical systems (MEMS). Computing elements can now have *sensors* to measure the physical world and *actuators* that initiate physical response. Whether such electro-mechanical systems operate actually at the nanometer scale, thus warranting the fashionable term "nanotechnology," is largely irrelevant.[14]

---

10. Imagine active RFIDs in our shoes fueled by the act of walking—through piezoelectrics that transduce physical vibrations into electrical energy. Of course, a cheap battery may outlast the average shoe.

11. *See, e.g.*, Auto-ID Labs, http://web.mit.edu/auto-id/www/index.htm (last visited Jan. 25, 2004) (discussing the electronic product code, a ninety-six bit number, embedded in RFID tags) (on file with the Washington and Lee Law Review).

12. Wal-Mart has announced that its top one hundred suppliers will be required to use RFID technology on cartons and pallets shipped to Wal-Mart by the end of 2004. Barnaby J. Feder, *How to Find That Needle Hopelessly Lost in the Haystack*, N.Y. TIMES, Sept. 29, 2003, at C1; *see also Gillette to Buy 500 Million EPC Tags*, RFID J., Nov. 15, 2002, *at* http://www.rfidjournal.com/article/articleview/115/1/1 (last visited Oct. 20, 2004) (noting Gillette's intentions to tag pallets and cases) (on file with the Washington and Lee Law Review). RFIDs have been inserted into cattle as well as the military equipment sent off to Iraq. *See* Gerald McNerney, *Radio Free Manufacturing*, Tech Update, *at* http://techupdate.zdnet. com/techupdate/stories/main/0,14179,2908740,00.html (Jan. 14, 2003) (noting that the Department of Defense is placing RFID tags on all assets shipped to the Persion Gulf region) (on file with the Washington and Lee Law Review).

13. Phillips Semiconductor, a leading manufacturer of RFIDs, claims to have shipped nearly one billion RFIDs as of November 2003. Mario Rivas, *RFID—Its Applications and Benefits*, RFID Privacy Workshop, 13, *at* http://www.rfidprivacy.org/papers/rivas/rivas.pdf (Nov. 15, 2003) (on file with the Washington and Lee Law Review). The Europeans are considering embedding RFIDs into banknotes. *See* Winston Chai, *Radio ID Chips May Track Banknotes*, CNETAsia, *at* http://news.zdnet. com/2100-1009_22-1009155.html (May 22, 2003) (noting that European Central Bank was concerned with counterfeiting and money-laundering) (on file with the Washington and Lee Law Review).

In a Buffalo, New York, charter school, children must wear RFID tags around their necks, allowing the school to track them when they enter the school. Eventually the system will track students' punctuality for every class. Julia Scheeres, *Three R's: Reading, Writing, RFID*, WIRED NEWS, *at* http://www.wired.com/news/technology/0,1282,60898,00.html (Oct. 24, 2003) (on file with the Washington and Lee Law Review).

14. Our colleague Greg Pottie notes that actuation—moving small motors, and the like—scales poorly with smaller size due to the increased role of friction. Also, extremely small devices are difficult to program and recover from the environment. Accordingly, in implementing PerC, a broad mix of differently sized devices will be necessary and useful:

More important is that these systems, small enough to be unobtrusive, can detect sight, sound, weight, pressure, heat, moisture, acceleration, electromagnetic radiation, or the existence of specific particulates.

After sensing this information, PerC can also initiate action by flipping a switch that can trigger micromotors. Real-life examples of MEMS technologies already exist: Automobile air bags are controlled by MEMS accelerometers that use as inertial elements a miniature cantilever. Professional tennis players use smart rackets, which intelligently translate the energy received by a ball's impact back into an "active counterforce" in the racket's throat as well as dampening countervibrations.[15]

What we can expect, then, are networks of miniaturized, wirelessly interconnected, sensing, processing, and actuating computing elements kneaded into the physical world. This animated control loop—of sensing data, processing it, then responding to it—can take place without direct human intervention or delay. In this sense, PerC can function automatically and, depending on its sophistication and one's definition, autonomously.[16] In sum, we offer the term "PerC" for the type of computing-communications that will emerge as the three trends of ubiquity, embeddedness, and animation converge in the next two decades.[17] It encompasses a gradual and familiar extension of

---

Smaller will not always be better.

15. Junko Yoshida, *Piezoelectric Rackets Add Professional Oomph*, EE TIMES, *at* http://www.eetimes.com/sys/news/OEG20020607S0077 (June 10, 2002) (on file with the Washington and Lee Law Review).

16. We are familiar with this sort of autonomous loop in the form of antilock braking systems (ABS) in our automobiles. Other automobile examples include dynamically adjusting steering. *See* Asad M. Madni & Roger F. Wells, *An Advanced Steering Wheel Sensor*, SENSORS, *at* http://www.sensorsmag.com/articles/0200/28/main.shtml (Feb. 2000) (describing steering position sensors that provide "vital information that helps detect and correct deviations between the driver's intended course and the actual course of the vehicle") (on file with the Washington and Lee Law Review).

17. Related terminology includes the "X Internet," coined by Forrester Research to talk about an Internet that is extended beyond the traditional PC (extended) and populated with applets (executables). George F. Coony, *My View: The X Internet*, FORRESTER RESEARCH, *at* http://www.forrester.com/ER/ Marketing/1,1503,214,FF.html (Oct. 2000) (on file with the Washington and Lee Law Review); Kathryn Smetana, *The "X Internet" and PANS: Technologies of the Future Connect Consumers and Possibly Their Identities*, 14 LOY. CONSUMER L. REV. 245, 246 (2002). Also, sometimes the technology that will make what we call "augmented reality" possible is called "Personal Area Networks" (PANs). Smetana, *supra*, at 248–49. We have also heard the terms "proactive computing," *see, e.g.*, Intel Corp., *Explanatory Research: A Future of Proactive Computing*, *at* http://www.intel.com/research/ exploratory (last visited Oct. 17, 2004) (stating that in "the proactive computing model, computers will anticipate our needs and sometimes take action on our behalf") (on file with the Washington and Lee Law Review), as well as "invisible" and "disappearing" computing, see, e.g., The Disappearing Computer Initiative, *at* http://www.disappearing-computer.net (last

how the Internet is already used, for example, to determine show times by browsing a website. Just expect to be doing this while driving to the mall, from your communicator, which is wirelessly connected to the Internet and your car's local area network. PerC also encompasses more novel forms, such as building climate control. This aspect of PerC is not captured so much by smartphones but by analogy to the ubiquitous electrical motor. As Mark Weiser, the founder of the field of pervasive computing argued, motors are embedded everywhere, doing countless different types of work, in specific contexts, with most of us entirely oblivious to their existence.[18]

To convey some of PerC's remarkable potential, we offer one last scenario. Imagine a remote site that merits monitoring for urgent safety-and-rescue operations. Perhaps hostages have been taken in a building, an earthquake has collapsed a parking structure, or a toxic spill has contaminated a field. Imagine distributing PerC elements into the area by spraying them through ventilation shafts, having them ride atop small robots, or dusting the polluted field from a helicopter. These PerC elements would be equipped with the appropriate sensors, for instance with the ability to sense human bodies—through weight, motion, and heat—or particular chemical pollutants. The computing elements are programmed to discover nearby elements and self-configure into a functioning network. Moreover, they can coordinate adaptively as the physical environment changes, for instance when a footstep crushes a handful of these elements. After reconfiguring, they process the information collected locally and then send along results. The signals hop from element to element until they reach the safety officers outside.

This scenario and others in this Article are not raw science-fiction, even if they evoke Steven Spielberg's *Minority Report*.[19] Support for this claim comes from the discipline of computer science itself, which is reorganizing in light of this future.[20] At the same time, we do not want to exaggerate, and

---

visited Oct. 17, 2004) (stating an intention to learn "how information technology can be diffused into everyday objects and settings") (on file with the Washington and Lee Law Review).

18. *See* Weiser, *supra* note 1, at 98 (discussing the twenty-two different motors in a typical automobile that a driver likely will never notice).

19. For a brief discussion of how distant the technologies suggested in the movie are from today, see generally Sean Captain, *Future Gear: Spielberg's Computer*, PC WORLD, *at* http://www.pcworld.com/howto/article/0,aid,102455,00.asp (July 22, 2002) (on file with the Washington and Lee Law Review).

20. Just recently, the field of "pervasive computing" seems on the cusp of explosion, at least as reflected by the relevant disciplinary journals. For instance, Deborah Estrin and other computer scientists recently suggested that pervasive computing has arrived as a legitimate field

we recognize that PerC faces substantial technological obstacles. For instance, PerC must often operate under severe resource constraints, in terms of power, bandwidth, and requirements of heat dissipation. In addition, because PerC will be embedded into physical artifacts with long lifetimes, such as buildings, these computing elements must themselves be durable and be able to interoperate with subsequently-added, heterogeneous elements, designed under new technologies. Such challenges raise important hardware and software questions that have been recently identified on a national research agenda.[21] Still, we believe it likely that these challenges will be substantially met within the next two decades.

As technological and cost obstacles disappear, various actors exercising control over their respective spheres of influence will incrementally implement this technology. On streets, for example, local governments will adopt surveillance-enabling PerC to enhance both personal and national security. In shopping malls, store owners will adopt PerC to provide consumers seductive offers. And individuals who can afford it will adopt PerC for the same efficiency, convenience, and sociocultural reasons that we have rapidly adopted mobile telephony and broadband Internet access.[22] In

---

of computer science. *See* Deborah Estrin et al., *Embedding the Internet*, COMMUNICATIONS OF THE ACM, May 2000, at 39–41 (discussing developments in ubiquitous computing and the coming revolution of embedded Internet devices). Also, the IEEE has just published the first issue of a new journal entitled *Pervasive Computing: Mobile and Ubiquitous Systems*, with an introductory editorial by the editor-in-chief exclaiming that "[s]omething big is clearly under way. Where will it take us?" Mahadev Satyanarayanan, *Catalyst for Mobile and Ubiquitous Computing*, PERVASIVE COMPUTING: MOBILE AND UBIQUITOUS SYSTEMS, Jan.–Mar. 2002, at 2. Also, relevant conferences have been meeting for the past few years: "UbiComp" will have its sixth conference on ubiquitous computing in 2004, and IEEE's "PerCom" will have its third conference on pervasive computing in 2005.

Recent massive governmental R&D funding decisions provide further evidence. The Center for Embedded Networking Sensing at UCLA was recently established as a National Science Foundation Science & Technology Center and received forty million dollars in funding. *See generally* Center for Embedded Networking Sensing, *at* http://www.cens.ucla.edu (last visited Oct. 18, 2004) (on file with the Washington and Lee Law Review).

21. The National Research Council recently studied networked systems of embedded computers to produce a research agenda for the field. Of the eight research themes, one concerned the "[i]ntegration of technical, social, ethical, and public policy issues." EMBEDDED EVERYWHERE, *supra* note 8, at 10. This paper fits within that theme.

22. The FCC reported that the number of mobile telephone subscribers increased roughly 10% in 2002 to 141.8 million, a penetration rate of 49%. FCC, REPORT 03-150, EIGHTH ANNUAL REPORT AND ANALYSIS OF COMPETITIVE MARKET CONDITIONS WITH RESPECT TO COMMERCIAL MOBILE SERVICES 31 (2003), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-150A1.pdf. Three years earlier, there were only 86 million subscribers (32% penetration). FCC, REPORT 00-289, FIFTH ANNUAL REPORT AND ANALYSIS OF COMPETITIVE MARKET CONDITIONS WITH RESPECT TO COMMERCIAL MOBILE SERVICES 4 (2000), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-00-289A1.pdf. The

other words, PerC will be adopted in a highly decentralized manner. A top-down governmental mandate demanding the total adoption of these technologies is neither likely nor necessary for widespread deployment.[23]

Once implemented, opting out of PerC will not be easy and will eventually be seen as Luddite. After all, who among us regularly opts out of electricity, paved streets, security cameras, bar codes, web cookies, or in places such as Los Angeles, even the automobile if we can afford one? Although it is true that people can sometimes avoid these aspects of modern urban life, long-term resistance is typically futile. The same will be true with PerC. In sum, decentralized economic, social, and cultural forces will lead to the widespread and significantly unavoidable adoption of PerC in the next two decades. We have less time than that to plan.

B. What's Really New

---

number of high speed Internet connections in the United States increased 55% in 2002, from 12.8 million to 19.9 million. *See* Press Release, FCC, Federal Communications Commission Release Data on High-Speed Services for Internet Access (June 10, 2003), *available at* http://www.hraunfoss.fcc.gov/edocs_public/ attachmatch/DOC-235274A1.pdf.

23. Of course, we can envision the state making certain critical components necessary, such as a "smart" identification card, for example in the form of a state driver's license. Since 9/11, legislation has been introduced that would require smart identification cards for some or all individuals in America. Those cards would include biometric authentication, such as fingerprints or retinal scans. *See, e.g.*, Robert O'Harrow Jr. & Jonathan Krim, *National ID Card Gaining Support*, WASH. POST, Dec. 17, 2001, at A1 (describing legislation introduced by Sen. Dianne Feinstein (D-California) and Sen. Jon Kyl (R-Arizona) that would require foreign nationals to have smart visa cards). Members of the military already carry these cards. *See id*. (reporting that approximately four million such cards are to be issued in the next two years). And such cards are quite popular globally. *See id*. (reporting that more than one hundred nations have national identification cards).

Support for national ID cards has weakened since peaking immediately after the September 11 attacks. *See* Julia Scheeres, *Support for ID Cards Waning*, WIRED NEWS, *at* http://www.wired.com/news/print/0,1294,51000,00.html (Mar. 13, 2002) (reporting that only 26% of Americans favored a national identification system, compared to 70% a week after the attacks) (on file with the Washington and Lee Law Review). Nevertheless, some members of Congress have continued to push for national ID cards. *See* Bureau of Nat'l Affairs, Inc., *GOP Policy Committee Looks to SSNs for Minimum State Licensing Standards*, 2 PRIVACY & SEC. L. REP. 1021, 1035 (2003) (noting efforts to establish uniform standards for state IDs and a state-to-state information system, which could be significant steps towards a de facto national ID card). For a summary of recent proposals for national ID cards, as well as arguments for and against them, see generally Neda Matar, *Are You Ready for a National ID Card? Perhaps We Don't Have to Choose Between Fear of Terrorism and Need for Privacy*, 17 EMORY INT'L L. REV. 287 (2003).

Now that we have defined PerC, we articulate its most significant qualities. In doing so, we distinguish between what is really new from the merely novel.

1. Geolocation Matters (Again)

Early enthusiasm about the Internet rested partly on obliterating space as a relevant dimension, thereby undermining the significance of physical location and distance. Numerous commentators have examined the political and jurisdictional implications of this phenomenon.[24] Some commentary is romantic exaggeration, to be sure: Location and distance have always mattered. That said, computing-communications have in certain ways undermined their significance. And, at first glance, PerC's ubiquity seems to contribute to the irrelevance of location. If exchanging information is the only point, and information can be exchanged from anywhere to anywhere, then it scarcely matters where one is physically located. As modern mobile telephone usage demonstrates, one need not be co-present to be in the same conversation.

The physical embeddedness of PerC will, however, reintroduce the significance, and at times the primacy, of physical space. Due to PerC's tight coupling with the physical world, it will increasingly matter where you are. Put another way, the functioning and experience of PerC will not be space-neutral; instead, PerC will pay attention to an individual's location. Users of Wi-Fi are already aware of the difference location makes: On one account, "Wi-Fi users are the most location-obsessed people on Earth."[25]

A concrete example illustrates this point. Regardless of where you are, accessing the *New York Times* online is largely a universal experience. Whether downloaded in New York or Los Angeles, essentially the same content is provided in the same manner. In this sense, NYTimes.com is space-neutral. It does not much matter where either client or server is physically located in this information exchange. To be sure, one can set geographical

---

24. *See generally* Paul Schiff Berman, *The Globalization of Jurisdiction*, 151 U. PA. L. REV. 311 (2002); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

25. *See* Paul Boutin, *Putting the World into the Wide Web: An Instant Messenger That Knows Where You Are*, SLATE, *at* http://slate.msn.com./id/2083733 (May 30, 2003) (describing new Wi-Fi technology that tells users when their friends are online and nearby—essentially "an AOL Instant Messenger that knows where you are") (on file with the Washington and Lee Law Review). Of course, this may just be a transitional phenomenon, until Wi-Fi becomes truly ubiquitous. The same could be said of notebook computer users and electrical outlets given the current state of battery technologies.

preferences that request NYTimes.com to personalize its content, such as weather reports, to one's location. But this is the exception not the rule.

With PerC, the exception becomes the rule. The individual's location at a fine level of granularity (much finer than zip code), via global positioning satellite (GPS), will be a datum that can be known automatically, without cumbersome manual entry, and constantly utilized.[26] For instance, when you enter the shopping mall, all friends in your social network who are nearby can be buzzed.[27] The fact that you are driving toward a particular freeway exit will determine what "points of interest," such as nearby restaurants (and their specials), are broadcast on your car's stereo.[28] When requesting a taxi, there will be no need to provide potentially inaccurate directions to your current location.[29]

These examples could be seen to emphasize personalization more than the primacy of location. And an individual's geographical position is undoubtedly a crucial datum for personalizing any information environment. But with PerC, the "personalization" is not only with respect to the individual but also

---

26. Location can be determined through mobile telephone tower triangulation, for example, with an accuracy of a few hundred feet in urban areas. HOWARD RHEINGOLD, SMART MOBS 95–97 (2002). Other techniques include GPS devices, or some combination of triangulation and GPS. *See* FTC, PUBLIC WORKSHOP: THE MOBILE WIRELESS WEB, DATA SERVICES AND BEYOND: EMERGING TECHNOLOGIES AND CONSUMER ISSUES, 4–6 (2002) [hereinafter FTC] (describing specific private sector implementations of such auto-location services), *available at* http://www.ftc.gov/bcp/reports/wirelesssummary.pdf; *see also* Jay Warrior et al., *They Know Who You Are: New Technologies Can Pinpoint Your Location at Any Time and Place. They Promise Safety and Convenience—But Threaten Privacy and Security*, IEEE SPECTRUM, July 1, 2003 (describing assisted GPS systems), 2003 WL 13280321.

The FCC has required commercial mobile radio service providers to implement E911 services, which by December 31, 2005 require location information accurate from 50 to 100 meters. *See* FCC, FCC WIRELESS 911 REQUIREMENTS 2–3 (2001), http://www.fcc.gov/911/enhanced/releases/factsheet_requirements_012001.doc (last visited Jan. 11, 2005) (describing requirements that mandate Automatic Locator Identification (ALI) technology for wireless providers which call for accuracy and reliability within 50 to 100 meters depending on the type of solution involved) (on file with the Washington and Lee Law Review).

27. *See, e.g.*, AT&T Wireless, *Find People Nearby*, *at* http://www.attwireless.com/ocs/featuresupport/organization/findfriendsqa.jhtml (last visited Oct. 18, 2004) (describing AT&T's mMode "Find People Nearby") (on file with the Washington and Lee Law Review); Invertix Corp., *mNET Applications*, *at* http://invertix.com/mnet_ applications.html (last visited Oct. 18, 2004) (describing mNET Friend Finder, by Invertix, which allows friends to locate each other based on location and presence) (on file with the Washington and Lee Law Review).

28. *Cf.* Warrior et al., *supra* note 26 (describing how one might use a GPS-enabled phone to locate the closest coffee shop).

29. *See, e.g.*, Tim Richardson, *Mobiles Hail London Cabs*, THE REGISTER, http://www.theregister.co.uk/2003/04/29/mobiles_hail_london_cabs (Apr. 29, 2003) (discussing location-based service that directly connects phone calling passengers with nearby available taxis) (on file with the Washington and Lee Law Review).

to the physical environment in which PerC is embedded. As a general matter, different environments, at different locations, will have widely different types of computing embedded, thereby subjecting their inhabitants to heterogeneous computing environments. For instance, an airport will have qualitatively different surveillance structures than a friend's home. At the other extreme, we can imagine vacation spots specifically designed with minimal PerC for those of us desperate *not* to "stay in touch," or night clubs that employ RFID jammers[30] to promote anonymity while providing access to other information, such as sexual availability.

Even within the same general environment, such as a university campus, PerC may operate in ways that pay attention to the place of embedding. For example, one might imagine computer-controlled gate systems that close if a civil disturbance is detected nearby. But each gate may respond differently to the inputs it senses. If a demonstration in one part of the campus has historically preceded a demonstration in another part of the campus, that precedent could be programmed into the sensors and processors embedded within the gating system. Through a form of place-profiling, the gate enclosing the business school might stay open, while the gate enclosing the ethnic studies department locks.

2. Digital Information Economics

PerC brings certain aspects of the information economics of cyberspace into real space. Back in 1998, one of us emphasized the qualitatively different threat to information privacy posed by cyberspace as compared to real space:

> [I]magine the following two visits to a mall, one in real space, the other in cyberspace. In real space, you drive to a mall, walk up and down its corridors, peer into numerous shops, and stroll through corridors of inviting stores. Along the way, you buy an ice cream cone with cash. You walk into a bookstore and flip through a few magazines. Finally, you stop at a clothing store and buy a friend a silk scarf with a credit card. In this narrative, numerous persons interact with you and collect information along

---

30. *See* Richard Shim, *Security Firm Aims to Ease RFID Concerns*, CNET NEWS.COM, *at* http://news.com.com/2100-1039_3-5068910.html (Aug. 27, 2003) (describing development of "blocker tags," which could be embedded in a watch, that would overflow RFID readers, thereby cloaking the value of nearby RFID tags) (on file with the Washington and Lee Law Review). The full technical paper is Ari Juels et al., *The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*, 2003 PROCEEDINGS OF THE 10TH ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 103. A successful implementation of this strategy requires "selective blocking," which in turn would require particular standards to be adopted in the underlying protocols used by RFID readers—no trivial task. *Id*. at 107–08.

> the way. For instance, while walking through the mall, fellow visitors visually collect information about you, if for no other reason than to avoid bumping into you. But such information is general—e.g., it does not pinpoint the geographical location and time of the sighting—is not in a format that can be processed by a computer, is not indexed to your name or another unique identifier, and is impermanent, residing in short-term human memory. You remain a barely noticed stranger. One important exception exists: The scarf purchase generates data that are detailed, computer-processable, indexed by name, and potentially permanent.
>
> By contrast, in cyberspace, the exception becomes the norm: Every interaction is like the credit card purchase. The best way to grasp this point is to take seriously, if only for a moment, the metaphor that cyberspace is an actual place, a computer-constructed world, a virtual reality. In this alternate universe, you are invisibly stamped with a bar code as soon as you venture outside your home. There are entities called "road providers," who supply the streets and ground you walk on, who track precisely where, when, and how fast you traverse the lands, in order to charge you for your wear on the infrastructure. As soon as you enter the cyber-mall's domain, the mall begins to track you through invisible scanners focused on your bar code. It automatically records which stores you visit, which windows you browse, in which order, and for how long. The specific stores collect even more detailed data when you enter their domain. For example, the cyber-bookstore notes which magazines you skimmed, recording which pages you have seen and for how long, and notes the pattern, if any, of your browsing. It notes that you picked up briefly a health magazine featuring an article on St. John's Wort, read for seven minutes a newsweekly detailing a politician's sex scandal, and flipped ever-so-quickly through a tabloid claiming that Elvis lives. Of course, whenever any item is actually purchased, the store, as well as the credit, debit, or virtual cash company that provides payment through cyberspace, takes careful notes of what you bought—in this case, a silk scarf, red, expensive.[31]

Soon, this distinction between real space and cyberspace will no longer stand. Widespread *embedding* of RFID tags will incorporate elements of the physical world into computer processable space: We will, in one sense, have digital cookies in a bag of oatmeal cookies. Not only will physical items, such as magazines that we flip through, have these tags; we as individuals will carry them, too. And through them, we will likely authenticate our identity to multiple queries of "who are you?" made by the enacted environment.

In other words, regular authentication will not require subcutaneous computer chips[32] or dystopian retina scanners posted on every street corner.

---

31. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1198–99 (1998).

32. *See* PRIVACY JOURNAL, at 1, http://www.privacyjournal.net/newsletter.htm (Feb.

Instead, our regularly carrying of numerous identification cards with built-in RFID tags is more likely how authentication will take place.[33] This includes the frequent shopper card that we carry voluntarily—inasmuch as every large grocery chain has such a card, and the prices are much higher without it. Or, a real space version of Microsoft's "Passport." Or, the widespread acceptance of a private smart card, which replaces cash and verifies identity.[34] If these cards can be read at a distance, then potentially every item we walk past or look at, much less buy, may be associated with our identity. And with ubiquitous access to databases, this information can be stored, processed, and shared, perhaps in real time.

The very same marketing incentives and economics that have prompted massive personal data processing in cyberspace will emerge in this digitalized real space. One no longer will need to be "logged on" to cyberspace in order for its data vacuum to suck up one's data trail. Detailed, computer-processable, individually-indexed, and permanent data may become just as collectible in real space as in cyberspace. Put another way, we might never be able to "log off"—when smart homes, always-on communication devices, GPS sensors in our cars, RFIDs in our tires[35] and our shoes,[36] and public safety scanners are tracking us always.

2003) (describing the work of a company called VeriChip, which has already implanted transponders on twenty Americans) (on file with the Washington and Lee Law Review).

33. Compare the Malaysian government's smart ID card, which contains 32KB of information. *See* Dan Farmer & Charles C. Mann, *Surveillance Nation: Part Two*, TECH. REV., May 2003, at 46, 50 (describing card system as sensibly designed to quarantine different types of data into different areas, such that access can be modulated). Other countries that have shown significant interest include China and Italy.

34. *See Japan Seeks Smarter Ideas for Smart Cards*, CNN.com, *at* http://www.cnn.com/2003/TECH/ptech/02/17/japan.smart.cards.ap/index.html (Feb. 17, 2003) (discussing the popularity of the Japanese Suica smart card, used by roughly half the possible users of the Tokyo subway system) (on file with the Washington and Lee Law Review).

35. Michelin is testing RFIDs embedded in automobile tires to facilitate identification and tracking. It reports successful reads from two feet away. *Michelin Embeds RFID Tags in Tires*, RFID JOURNAL, http://www.rfidjournal.com/article/view/269 (Jan. 17, 2003) (on file with the Washington and Lee Law Review). Active IDs that sense air pressure and temperature are also being developed. *Id.*

In mass media coverage, it is often noted that Michelin is doing this to comply with the Transportation Recall Enhancement, Accountability, and Documentation (TREAD) Act, Pub. L. No. 106-414, 114 Stat. 1800 (2000) (codified as amended in scattered sections of 49 U.S.C.). Passed in the wake of the Firestone tire recalls, the TREAD Act updates the National Traffic and Motor Vehicle Safety Act of 1966, Pub. L. No. 89-563, 80 Stat. 718 (1966) (codified as amended at 49 U.S.C. §§ 30101–30169 (2000)). The Act makes no specific mention of RFID technologies. It does, however, require early notification of any potential problems to the National Highway and Transportation Administration, 49 U.S.C. § 30118(c) (2000), and data collection necessary to discharge such reporting requirements could be facilitated by RFIDs.

3. Deep Invisibility

Early investigations on the role of technology in society, such as Marshall McLuhan's study of media, demonstrated how pervasiveness can recede into cognitive invisibility.[37] Technologies that have fully matured and have become culturally accepted retreat into the unnoticed, invisible background. Take, for example, the rather odd technology of eyeglasses, which involves taking two lenses, framing them, and perching them on top of our nose and ears—a primitive form of sensory augmentation. Yet, we pay little attention to eyeglasses most of the time.[38]

PerC will be the same—but more so—because a principal design feature is to have computing recede into the background. Mark Weiser asked us back in 1991 to imagine a world in which computing simply disappeared.[39] He compared computing to writing, another revolutionary information technology. Writing is everywhere—on computers, billboards, signs, even candy wrappers. But writing no longer seems like a technology. We take writing for granted; it does not demand our attention in the same way that a computer does, with its clumsy user interfaces. The same could happen with computing.

The TREAD Act also requires manufacturers of recalled tires to have some plan to prevent resale of those tires. *See id.* § 30120(d) (2000) (requiring that a "manufacturer . . . file with the Secretary a copy of the manufacturer's program under this section for remedying a defect or noncompliance"). RFID authentication could help in this requirement, too. Finally, the Act envisions a future tire pressure warning system that notifies the driver of dangerously low tire pressure. TREAD ACT, Pub. L. No. 106-414, § 13, 114 Stat. 1800, 1806 (2000) (not codified, appears in 49 U.S.C. § 30123 notes). RFID sensors could be used to implement such a system. For a useful summary of the Act, see generally Kevin M. McDonald, *Don't TREAD on Me: Faster Than a Tire Blowout, Congress Passes Wide-Sweeping Legislation That Treads on the Thirty-Five Year Old Motor Vehicle Safety Act*, 49 BUFF. L. REV. 1163 (2001).

36. *See, e.g.*, Sean Captain, *Future Gear: Tiny Chips, Everywhere*, PC WORLD, *at* http://www.pcworld.com/howto/article/0,aid,106403,00.asp (Oct. 30, 2002) (discussing the possibility of a passerby using a PDA to determine the brand of your shoes by reading their RFID signal (relating an interview with Paul Mackinaw of Accenture Technology Labs)) (on file with the Washington and Lee Law Review).

37. In a 1969 *Playboy* interview, McLuhan stated that when "a new media-induced environment becomes all-pervasive and transmogrifies our sensory balance, it also becomes invisible." ESSENTIAL MCLUHAN 237 (Eric McLuhan & Frank Zingrone eds., 1995).

38. Another example is the ubiquitous telephone pole, which carries multiple communications and power lines. Generally, we edit them out of our visual field.

39. *See* Weiser, *supra* note 1, at 104 ("Machines that fit the human environment instead of forcing humans to enter theirs will make using a computer as refreshing as taking a walk in the woods.").

Equally important, in many PerC applications the computing elements are not designed to interface directly with any human user.[40] Instead, PerC interacts directly with the physical environment that only indirectly affects its human inhabitants. If we consider in addition PerC's embedded nature, we may achieve a sort of "deep" invisibility. The embedded computing elements will be too small to see or will be installed in ways that are not noticeable, even when we are looking for them.[41] There will be, for instance, no wires along which the communications travel. Seen in this light, the proper analogy is no longer eyeglasses but contact lenses.

4. Augmented Reality—the Percolated Person

The first three characteristics of PerC describe tangible, if difficult to imagine, transformations within technology and society. Our final two observations about PerC operate at a higher level of abstraction. We believe that a new, important aspect of PerC is to fortify a person's sensory, communicative, and processing powers, which will provide what some have called "augmented reality."[42] As Weiser pointed out, the goal of PerC is *not* an ever more realistic, *Matrix*-like virtual reality—where we immerse ourselves into a simulacrum of the real world, constructed on a computer server, and represented to our senses through goggles, earphones, and force-feedback suits. Instead, the goal is the very opposite—to embed computing into reality, to create a form of "embedded virtuality." In this world, computing is in the air, in the walls, in our sunglasses.

---

40. *See* EMBEDDED EVERYWHERE, *supra* note 8, at 28 (noting that because the computing elements are so tightly coupled with the physical world, individuals are not likely to think they are interacting with a computer but rather with the object with which it is coupled).

41. CASPIAN, a consumer group highly critical of RFID tags, has pointed out how large tags can be hidden in cardbox boxes, rolled up inside shampoo bottle tops, and placed between layers of paper packaging. It also points out examples of chipless tags, such as Inkode's system of embedding fine metal fibers into paper, which produces a unique radio "signature" that can be later identified. *See* Katherine Albrecht, *Privacy and Societal Implications of RFID*, RFID Privacy Workshop, Nov. 15, 2003, at 7–21 (describing how RFID tags can be integrated into products and their packaging so as to be virtually unnoticeable by consumers), *available at* http://www.rfidprivacy.org/2003/papers/albrecht.pdf (on file with the Washington and Lee Law Review). *See generally* Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), *at* http://www.spychips.com (last visited Oct. 19, 2004) (on file with the Washington and Lee Law Review).

42. Howard Rheingold attributes this phrase to a 1991 article by Walter Robinett. *See* RHEINGOLD, *supra* note 26, at 84.

In the ideal PerC implementation, no one lugs around a laptop looking for an outlet and data jack. Instead, computing is simply available, like digital oxygen, with effortless, invisible, seemingly natural access to data and information processing ability. To play out a scenario, consider a morning commute ten years from now. Leaving home as planned at 7:30 in the morning, your mobile communicator informs you of the morning traffic report, and on that basis, suggests the fastest route to your office, which is mapped out on your windshield. On your way, nonspam emails received since last night are read to you, and the speech recognition system in the car's computer relays your responses. As you pass by a commercial center, you receive a visual note on your dashboard that your favorite brand of shoes is on sale, with four styles in your size; they can be put "on reserve" simply by saying, "Computer, accept offer." Only a little more ubiquity in wireless access, better integration of databases, and a decrease in production costs are necessary to make this scenario reality.

By being bathed in such data, we augment our experience of reality with layers of contextually relevant information. It is as if human beings were granted an additional "sense" in addition to sight, hearing, taste, smell, and touch—a sort of sixth sense, a *datasense*. Preliminary implementations of such augmented reality already exist. For instance, contractors can walk through construction sites with a visor[43] that paints a digital overlay of the approved architectural drawings on the building in progress.

So envision a future where we can "right click" on any object with our communicators and receive contextually relevant information. People already "Google" each other before going on dates or to interviews. Think about having the option of one-click "Googling" anyone you walk past, *as you walk past*. PDA-sized gadgets that provide this sort of datasense about fellow conference attendees have already rolled out.[44] This process could become automated; no specific "request" to pull information will be required. Rather, software will manage our datasense and constantly seek out and filter information about nearby people. Consider how a parent might respond when she hears in her ear bud "Warning: Registered sex offender within fifty feet."[45]

---

43. For some description of visual overlays using headmounted displays, see *id*. at 92.

44. *See, e.g.*, Shockfish SA 2, Spotme Brochure, *at* http://www.spotme.ch/presskit/SPOTMEBrochure.pdf (last visited Nov. 16, 2004) [hereinafter Spotme Brochure] (describing "radar" function, which identifies name, photograph, and other biographical details of all people within thirty meters) (on file with the Washington and Lee Law Review).

45. Many states currently make information about sex offenders available on the Internet. For a list of the sex offender community notification laws in every state, see *Megan's Law by*

The above examples involved collecting information by authenticating an individual's identity and referencing it to extant databases. But PerC's animation—its sensing powers in particular—could allow our *datasense* to collect types of information previously unavailable. For instance, sensors could collect infrared data, which can speak volumes. A childcare center may strictly prevent drop-offs of children with fever. An employer may guess that a job applicant is pregnant. A border official may profile visitors for SARS.[46]

Everything said above about people could also apply to things and places. Is that a real Gucci bag or an imitation? A cloth logo is much easier to forge than an encrypted digital signature embedded in the manufacturer's RFID. What is the accident history of this plane I am about to board?[47] Why is my neighbor's house registering such high infrared readings? Are there hot tubs, or as in the case of *Kyllo v. United States*,[48] a marijuana growing operation? A walk around the neighborhood could provide telling reconnaissance.

Here, we point out that augmenting the realities of individuals through PerC could have unexpected consequences on state power. In *Kyllo*, the question presented was whether law enforcement's thermal imaging scan of a house constituted a "search" for purposes of the Fourth Amendment. The Supreme Court held that this "sense-enhancing technology" was in fact a search; accordingly, the police needed a warrant before "reading" a house

---

State, KLAAS KIDS FOUND., *at* http://www.meganslaw.org (last visited Oct. 19, 2004) (on file with the Washington and Lee Law Review). For a summary of the history of these laws, as well as the ultimately unsuccessful constitutional challenges, see generally Kimberly B. Wilkins, *Sex Offender Registration and Community Notification Laws: Will These Laws Survive?*, 37 U. RICH. L. REV. 1245 (2003).

46. During the SARS epidemic, Singapore used infrared cameras, capable of sensing temperature at a distance, to check travelers in the airport for fever as they entered or left the country. Richard C. Paddock, *A Hotbed of SARS Warfare: Mass Temperature Testing Is Just One of the Tools That the Autocratic City-State of Singapore Is Wielding in Its Winning Assault on the Disease*, L.A. TIMES, May 8, 2003, at A1, *available at* 2003 WL 2403683.

47. The FAA files a detailed report for every incident involving damage to a plane or injury to a passenger, which is available by plane registration number, at https://www.nasdac.faa.gov/pls/nasdac/NASDAC.wwa_app_module.show?p_sessionid=148618 (last visited Oct. 19, 2004) (on file with the Washington and Lee Law Review). The age and engine type of the plane is available at http://162.58.35.241/acdatabase/acmain.htm (last modified Aug. 23, 2004) (on file with the Washington and Lee Law Review). Imagine such applications for amusement park rides.

48. Kyllo v. United States, 533 U.S. 27 (2001). For a thoughtful analysis of *Kyllo*'s significance, see David A. Sklansky, *Back to the Future:* Kyllo, Katz, *and Common Law*, 72 MISS. L.J. 143 (2002).

with a thermal imager.[49] However, the Court noted that this judgment was based in part on the fact that "the technology in question is not in general public use."[50] As PerC goes mainstream, thermal imagery and other forms of sensing could become sufficiently "mainstream" technology so as not to constitute a "search" in Fourth Amendment terms. If everyone has x-ray vision, so can the police, and everything will be in plain view.

5. Enacted Environments—the Percolated Place

Just as PerC can augment an individual's ability to sense, remember, analyze, and react, it can empower the physical environment similarly. Thus, another metaphor through which we can understand the embedded and animated facets of PerC is a digital nervous system grafted into the material world. In many cases, that digital nervous system will allow the environment to respond, in real time and without human intervention, to the sensed circumstances. These networked systems may also have the capability to learn and to adapt to new information or conditions.

The simple fact that computing "in the air" will directly lead to changes in the physical environment is significant. After all, mistakes are inevitable, which raises not only questions about the probability and magnitude of harm but also moral and legal liability.[51] More interesting, this kind of environmental responsiveness may rise to the level of autonomous behavior, or, perhaps almost as important, its strong impression.[52] Will we be concerned

---

49. *Kyllo*, 533 U.S. at 40.

50. *Id*. at 34.

51. *See, e.g.*, CURTIS E.A. KARNOW, FUTURE CODES: ESSAYS IN ADVANCED COMPUTER TECHNOLOGY AND THE LAW 138 (1997) (pointing out that artificial intelligence systems will inevitably create harm). Karnow argues that distributed artificial intelligence systems will undermine traditional notions of cause and effect in tort law. Accordingly, he recommends a quasi strict liability arrangement called the "Turing Registry." *See id*. at 178–86 (describing the Turing Registry as an insurance system where "risk would be assessed along a spectrum of automation: the higher the intelligence, the higher the risk, and thus the higher the premium").

52. If the environment responds quickly in cause-and-effect-like ways to shifting circumstances, we will likely impute to the environment traditional notions of agency. In fact, this is how we impute conscious will to our own behavior. *See generally* DANIEL M. WEGNER, THE ILLUSION OF CONSCIOUS WILL 14–15 (2002) (describing the difference between *phenomenal* will (the feeling of) and *empirical* will (actual causal mechanism) and how we often infer incorrectly the latter from the former).

that the room or street is tracking our every move, even if no human being is directly involved? How will we react when the environment misreads us, making wrong assumptions about who we are and what we want? For instance, how will we interpret billboards that change their image, perhaps in offensive ways, when we walk into its visual frame?[53]

As the environment itself gains a subject-like status, it can transform an individual's own experience of subjectivity. Compare Jeremy Bentham's Panopticon,[54] extensively discussed by Foucault,[55]—a physical space designed to exercise surveillance power and agency over its prisoners. The radial space of the centrally controlled prison embodied and, we might say, performed the order it imposed on the inmates. PerC portends far more such constructions.

Interesting examples of enacted environments have not yet been fully realized. However, some conceptual and partially implemented projects merit mention, particularly those by the architectural firm of Diller + Scofidio. Consider, for instance, their Blur Building from the Swiss Expo 2002 on Lake Neuchatel, which, as it was conceived, is an excellent case for architecture's role in the percolated public sphere.

---

53. Imagine simple-minded profiling on the basis of last name authenticated by ID cards that generate Chinese language advertisements to a person named "Kang" who is neither ethnically Chinese nor can read Chinese. What will others who share the environment and notice the advertisement infer? Or, what if two young men sidle up to you, and the billboard that you were watching quickly changes into a condom ad? Or a bail-bondsmen ad?

The beta service of G-mail, Google's free email service, which embeds advertisements on the basis of the e-mail's contents has already raised similar questions in a purely cyberspace context. *See, e.g.*, Saul Hansell, *The Internet Ad You Are About to See Has Already Read Your E-Mail*, N.Y. TIMES, June 21, 2004, at C1 (describing an ad placement about cellulite based on a college reunion email stating that it was "[g]reat seeing you and your wife").

54. In 1791, Jeremy Bentham proposed this prison design. In 1829, it was implemented in the Philadelphia Eastern State Penitentiary. Prisoners, who lived in solitary confinement, could be seen by the guard but could not see themselves, the guard, or any other inmate. *See* Farmer & Mann, *supra* note 33, at 52 (describing Bentham's "panopticon, a domelike prison where guards could observe all inmates at all times from within a central observation tower").

55. *See* MICHEL FOUCAULT, DISCIPLINE & PUNISH: THE BIRTH OF THE PRISON 201 (Alan Sheridan trans., Vintage Books 2d ed. 1995). Focault wrote:

> Bentham laid down the principle that power should be visible and unverifiable. Visible: the inmate will constantly have before his eyes the tall outline of the central tower from which he is spied upon. Unverifiable: the inmate must never know whether he is being looked at at any one moment; but he must be sure that he may always be so.

Id.

Photo Credit: Professor Dana Cuff

Blur Building

This building, with no function other than to be explored, is a steel structure perforated by more than 30,000 misting jets. The resultant fog produces an effect that the architects intended to blur the visual in order to heighten the experiential and tactile.

To continue to heighten realms of nonvisual information, Diller and Scofidio conceived of the "braincoat" that each visitor would wear into the structure. The braincoat, embedded with sensors and keyed to computer-coded information garnered from questionnaires filled out by each visitor, would trigger interactive responses by the building, generating identity- and location-specific experiences of the physical space. The architects imagined that the building's ability to track an individual would raise awareness of new technologies' potentials. As Liz Diller commented, "The building always knows where you are and who you are—the tracking makes the building omniscient."[56] Though the architects emphasized individual experience, they hinted at the possibilities of the building and braincoat's ability to construct collective identity among visitors, connecting one visitor to another or in some manner displaying the present occupants' collective features.

56. ELIZABETH DILLER & RICARDO SCOFIDIO, BLUR: THE MAKING OF NOTHING 173 (2002).

Photo Credit: Professor Dana Cuff

Visitors in Raincoats

Although the braincoats were never realized, replaced by everyday plastic raincoats, the possibility reveals a provocative notion of public space. In the Blur Building, PerC's potentials become apparent not only to track us pervasively, but also to join us at a particular moment to a nearby stranger or group, or, depending upon the information available to the system, to reveal ourselves within the public sphere.

These descriptions sharpen the difference between PerC scenarios that emphasize augmented reality on the one hand versus enacted environment on the other. Recall the augmented reality commuting example. The enacted environment version of that commute looks different. This time, you get a late start and leave home at 7:45 with barely enough time to make it to the office. As you race onto the freeway, a remote speed-limiting device prohibits your accelerator from going ten miles over the 55 MPH limit, and sensors on your bumper hold you back from tailgating. Based on your speed, acceleration, and frequency of lane changes, as measured by road sensors, your vehicle's exterior paint turns bright red,[57] warning other drivers that you are driving erratically. Signals are also sent to local law enforcement, depending on the degree and duration of your aggressive driving. As a courtesy, the audio system warns you that the police have been alerted. At the same time, civil fines are deducted from your bank account.[58] This scenario may seem like science fiction, but it may not be that far off.

Augmented reality and enacted environment are neither independent nor mutually exclusive forms of PerC. Indeed, the degree of augmentation of an individual's reality will depend on the environment, how enacted it is, what it

---

57. *See, e.g.*, Barnaby J. Feder, *A Glimpse of a Future in a New Kind of Light*, N.Y. TIMES, Feb. 11, 2003, at C1 (describing the technology of light-emitting microchips, with remarkable potential for brightness and energy efficiency).

58. Already, the city of London has used its extensive system of video cameras to charge owners of cars that enter restricted areas of the central city a substantial daily fee. Randy Kennedy, *The Day the Traffic Disappeared*, N.Y. TIMES MAG., Apr. 20, 2003, at 42–43; *see also* Farmer & Mann, *supra* note 33, at 50 (describing "feature creep" of the auto anticongestion technologies being used for anticrime and terrorism purposes).

permits or forbids, and what it encourages or discourages. In this way, the percolated person and the percolated place mark overlapping emphases in PerC's evolution. They can and will co-exist, compete, and adapt to each other as pervasive technologies evolve.[59]

III. The Public Sphere

So far, we have described salient aspects of PerC, a near-future set of technologies that will transform society. We do not believe that a global judgment about PerC's impact, either positive or negative, is helpful. Instead, we seek to understand its consequences by exploring its implications in a specific context. Our choice is the "public sphere," which is especially relevant given PerC's physical embodiment and influence on space.

A. The Public Sphere Described

A vast literature has accumulated, particularly in the past forty years, about the public sphere. Variously termed public space, civic space, public domain, open space, or public realm, the term "public sphere" connotes the comprehensive intermingling of spatial and social terrains. From the sociological literature, we take public sphere to mean a socio-spatial ground recognized as open to, accessible by, and shared among society's diverse members in their multiple roles as individuals, community members, consumers, and citizens. The public sphere stands in contrast to the private sphere—an intimate, protected, and familiar realm whose terms of access are established and controlled by the individual, to be shared among family and friends. To be more specific, the public sphere has the following four qualities.

First, it is accessible to diverse members of society. Second, it affords those individuals the opportunity of multiple uses: The public sphere is where cultural, political, commercial, and social life intersect and commingle in meaningful if not equal proportions.[60] Third, the public sphere engenders

---

59. As for timing, we believe that we will see substantial implementations of augmented reality within ten years. For example, Gartner Consulting predicts that 75% of teenagers will use wearable computing by 2010. RHEINGOLD, *supra* note 26, at 105. We believe we will see enacted environments within twenty years.

60. Given this view, we do not criticize malls that introduce nonretail services, such as government offices, community centers, and places of worship, as a cynical attempt simply to increase the number of shoppers. The access to such services may increase the number of mall

some form of exchange among participants. Thus, active participation is part of the scene, which can range from political protest to shopping. Fourth, and tightly connected to the prior features, such opportunities and interactions within the public sphere are recognized as such. This includes a visible sense of shared experiences among strangers.

As we see it, then, the public sphere is a collusion of physical space with the everyday world. It is where much of collective life, in its complexity and richness, happens. But the public sphere also serves more specific functions, whose value has been amply demonstrated by scholars such as Gerald Frug,[61] Richard Sennett,[62] and Benjamin Barber.[63] Drawing generally on these theorists, we believe that by being a space open to individuals in their multiple roles as community members, consumers, employees, passersby, and citizens, the public sphere fosters social interactions of both confrontation with otherness and shared experiences that facilitate a communal sensibility overall.[64] Notwithstanding attempts to create homogeneous living environments, we exist in a diverse and pluralist society. Thus, the public sphere de facto encourages chance interactions among strangers who may indeed seem quite strange to each other. In turn, such interaction ideally encourages curious discovery of the alien while promoting a tolerance for difference.

Because the public sphere tolerates and often encourages multiple roles for individuals—as consumer and citizen—it also functions as a staging ground for civic and political discourse. Opportunities for and performances of such dialogue can produce the civic engagement, recognized sense of community, and substantive deliberation necessary to a well-functioning democracy.[65] In noting this aspect of the public sphere, we risk privileging a

---

visitors, but by offering such services, the mall becomes more of a public sphere.

61. *See, e.g.*, GERALD E. FRUG, CITY MAKING: BUILDING COMMUNITIES WITHOUT BUILDING WALLS 117 (1999) (stating that public space, "because it is open to anyone whatsoever, provides exposure to opinions and culture very different from one's own"); Curtis J. Berger, Pruneyard *Revisited: Political Activity on Private Lands*, 66 N.Y.U. L. REV. 633, 637–48 (1991) (explaining the need for modern public forums, as explained in the legal and political science literature). "Public forums" as a First Amendment doctrinal term of art is not identical to the term "public sphere," as we have defined it; nevertheless, these ideas are closely related and certainly all public forums in the former sense would count as public spheres in the latter.

62. *See generally* RICHARD SENNETT, FALL OF PUBLIC MAN (1976) (discussing the public sphere from an historical perspective).

63. *See* BENJAMIN R. BARBER, STRONG DEMOCRACY: PARTICIPATORY POLITICS FOR A NEW AGE 151–55 (1984) (arguing that strong democracy requires the symbiotic relationship between community and participation that creates public ends).

64. *See generally* HANNAH ARENDT, THE HUMAN CONDITION (1959).

65. *See generally* FRUG, *supra* note 61.

vague ideal of deliberative democracy and denigrating other forms of social exchange, from exhibitionism to confrontation, observation to commerce. We resist such a romantic understanding of the public sphere,[66] and emphasize that not everyone need be engaged in Madisonian debate. People-watching,[67] not self-governance, may be what is on the agenda.

How and where is this "public sphere" realized today? Our definition of public sphere with its emphasis on recognized accessibility may imply a magnetic, central place such as a civic plaza downtown. But in the contemporary metropolis, the public sphere is both intentional and inadvertent, traditional and unconventional. It comprises the formal space of public squares and libraries, but also the more informal terrain of laundromat, elevator lobby, and the line outside the movie theatre. Marginal, territorialized, and unattractive realms can also fit the definition. The public sphere should not be seen as necessarily fixed because such a view privileges permanence over more dynamic forms including temporary space, such as a traffic jam or a hot dog vendor's cart; events, such as street theatre or an arrest; and unfixed or mobile space, such as a city bus.

Also, the public sphere is not limited to publicly-owned property.[68] This was more often the case in the pre-industrial city, where public space was the symbolic and actual center of the city, reminding citizens of their collective obligations and privileges.[69] But the contemporary public sphere is much less clearly located because it occupies spaces that may be privately-owned, such as the space between the front porch and the sidewalk, the shop window, the farmers' market, and the private school playground. To be sure, certain privately-owned spaces may have fewer indicia of a public sphere because their territory has been, for instance, limited in terms of general access—no public transportation to the upscale mall—or flattened in terms of potential uses—no political leafleting. Implicit here is the notion that the "public sphere" in its practical realization may stray far from the ideal.

---

66. *See generally* MAARTEN HAJER & ARNOLD REIJNDORP, IN SEARCH OF NEW PUBLIC DOMAIN: ANALYSIS AND STRATEGY (2001).

67. *See, e.g.*, LYN H. LOFLAND, THE PUBLIC REALM: EXPLORING THE CITY'S QUINTESSENTIAL SOCIAL TERRITORY 77–98 (1998) (discussing aesthetic and interactional pleasures of the city).

68. *See* Berger, *supra* note 61, at 655–56 (arguing that what counts as "public" versus "private" spaces is not determined exclusively by public or private ownership of property).

69. *See generally* ANASTASIA LOUKAITOU-SIDERIS & TRIDIB BANERJEE, URBAN DESIGN DOWNTOWN: POETICS AND POLITICS OF FORM (1998) (detailing the evolution and decline of American downtowns).

B. The Public Sphere Malled

Citing myriad causes, scholars from various disciplines have decried the decline of the public sphere. For example, sociologist Richard Sennett elucidates the retreat since the Industrial Revolution from civility to intimacy, from the cosmopolitanism of urbanity to an obsession with private life.[70] By contrast, the social philosopher Jürgen Habermas believes that the public sphere and its core of rational public reasoning have declined because of the rise of mass media and the manipulative mass culture that it ushered in.[71] Some planners suggest that fear and perceptions of crime have intimidated people enough to restrict their use of public space.[72]

Whatever the causes, such decline is not an inevitable process of nature. The public sphere is a social construction—amenable to direct action by individuals, groups, and societies.[73] Put another way, the public sphere—including the architecture, social norms, and legal parameters[74] that constitute its foundation—are objects of social choice. Open spaces, for instance, can be designed so that they are more or less public. And while physical design does not dictate particular behavior, it can encourage or discourage certain activities.

Indeed, many cities are going to great expense to remake themselves to encourage public life. The "village" or New Urbanist model would expand the width of sidewalks and increase their commercial activity while calming vehicular flow in the center city to encourage pedestrians. Closed circuit TV cameras monitor street life so that the actual rate of crime as well as its public perception are reduced. PerC will add another layer to the environmental matrix that can be manipulated within the public sphere. As we percolate the

---

70. *See generally* SENNETT, *supra* note 62 (discussing the public sphere from an historical perspective).

71. Sylviane Agacinski, *Stages of Democracy*, *in* PUBLIC SPACE AND DEMOCRACY 129, 129 (Marcel Hénaff & Tracy B. Strong eds., 2001); Dana R. Villa, *Theatricality in the Public Realm of Hannah Arendt*, *in* PUBLIC SPACE AND DEMOCRACY 144, 161 (Marcel Hénaff & Tracy B. Strong eds., 2001).

72. LOUKAITOU-SIDERIS & BANERJEE, *supra* note 69, at 180.

73. *See, e.g.*, Marcel Hénaff & Tracy B. Strong, *The Conditions of Public Space: Vision, Speech, and Theatricality*, *in* PUBLIC SPACE AND DEMOCRACY 1, 5 (Marcel Hénaff & Tracy B. Strong eds., 2001) (noting that public space is "a human construct, an artifact, the result of the attempt by human beings to shape the place and thus the nature of their interactions").

74. Of course, these modalities of governing behavior have been articulated famously by Larry Lessig. *See, e.g.*, Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 507–14 (1999) (identifying these three and the market as four principal modalities).

physical environment, we intentionally or inadvertently redesign the public sphere. In doing so, we will either catalyze or inhibit its primary functions.

So far, we have narrowed the question down to: "What impact will PerC have on the public sphere?" But this question is still too abstract and needs a concrete place for application. Accordingly, we focus on a specific, familiar space: the various forms, both formal and informal, of the shopping mall. After all, in many urban environments, malls are arguably what our public spaces have become. The accessible, open space of the street has been ingested by shopping malls, which in turn have invaded most urban spaces, from airports to museums. We should not be surprised when urban social critics contend that the entire world has become a mall.[75] At the same time, according to Benjamin Barber, this malling of America has "mauled" civil society.[76] In these spaces, the logics of consumption have supplanted any larger mandates of the public interest. The shopping mall thus threatens the public sphere not only physically—in the sense of absorbing all public space—but also socio-culturally—by foregrounding a particular ideology of shopping and consumption, which frames the individual as first and foremost a consumer.

Notwithstanding this harsh portrayal, we recognize the mall's latent potential to be a meaningful public sphere. Given the malleability of shopping as a practice and its sensitivity to changes in underlying technologies, we must remember that the shopping mall holds forth the constant possibility of reinvention and reconstruction. That transformation can make the shopping mall more or less like an ideal public sphere. Further, we seek to be practical and look at the spaces where people actually are, not where academics long for them to be.[77] For these reasons, the mall, defined capaciously, makes for a perfect site of investigation.

If situating our analysis of PerC in the shopping mall seems frivolous or forced,[78] consider the public/shopping convergence represented by the Prada

---

75. *See generally* VARIATIONS ON A THEME PARK: THE NEW AMERICAN CITY AND THE END OF PUBLIC SPACE (Michael Sorkin ed., 1992).

76. *See* Benjamin R. Barber, *Malled, Mauled, and Overhauled: Arresting Suburban Sprawl by Transforming Suburban Malls into Usable Civic Space*, *in* PUBLIC SPACE AND DEMOCRACY 201, 202–03 (Marcel Hénaff & Tracy B. Strong eds., 2001) (decrying "McWorld" as having converted "multiuse public space into a one-dimensional venue for consumption").

77. *See, e.g.*, Jennifer Niles Coffin, *The United Mall of America: Free Speech, State Constitutions, and the Growing Fortress of Private Property*, 33 U. MICH. J.L. REFORM 615, 617–18 (2000) (focusing on the mall as a place that provides far more than simple shopping).

78. Another response could be that this focus is irrelevant because real-space shopping sites will be entirely supplanted by cyber shopping. Even as more and more purchases are made online, there is little reason to think that physical sites for shopping for goods and services will

Flagship Store in New York, which was designed by Rem Koolhaas/OMA and opened in December 2001. The *New York Times* architecture critic called it "a model block of intelligent optimism about urban life."[79]

The full-block store is organized as an interior street, called the Wave by the architect[80] with a set of metal boxes floating above for the few products displayed in this new form of nomadic shop window. The vast space is open for walking, watching, and less apparently, buying. Instead, Prada uses architecture in conjunction with digital technology, to create urban identity and branding. The store has become a public event, aided by in-store technology.[81] This includes glass dressing rooms that phase-change from transparent to opaque, large video screens that replace store mirrors to show your back and side views "live," data banks like ATM machines that check inventory, and a series of embedded sensors that track what you take into the dressing rooms.[82] Within the dressing rooms are smart closets that read a garment's RFID tag to display additional details, possible accessories, similar items with the same look, and how it looks modeled on the runway.[83] Prada is considering additional technologies, including scanners that charge the customer automatically when a customer carries a product out the door.[84]

What, then, will PerC do to and for malls that may signal both the end of the public sphere and its last, best fighting chance? We have two stylized stories to tell. On the one hand, the tale of the "smooth mall" is one of a perfected, lubricated medium for ultimate shopping, bathing us in Siren calls we cannot refuse. On the other hand, the tale of "friction mall" is one of political shopping supported by peer-to-peer engagements and confrontation.

---

disappear; they serve too many functions that computer-mediated shopping cannot quite yet satisfy, such as trying on clothes or dining out. This is not, however, to denigrate or minimize the possibility of engineering public spheres in computer-mediated communities. *See generally* Jerry Kang, *Cyber-race*, 113 HARV. L. REV. 1130 (2000) (discussing ways to build online communities to pursue particular racial projects, such as integration). Indeed, we should pay attention to the public sphere qualities of spaces in both the physical and virtual worlds.

79. Herbert Muschamp, *Forget the Shoes, Prada's New Store Stocks Ideas*, N.Y. TIMES, Dec. 16, 2001, at ST1.

80. A photo of the store is available at http://www.classic.archined.nl/sites/RemKoolhaas_source page_e.html (on file with the Washington and Lee Law Review).

81. *Learning from Prada*, RFID J., June 24, 2002, *at* http://www.rfidjournal.com/article/articleview/272/1/79 (on file with the Washington and Lee Law Review).

82. *Id.*

83. *Id.*

84. Muschamp, *supra* note 79, at ST6.

IV. Embedding the Public Sphere

A. Smooth Mall

There is a science to mall design.[85] Malls are architecturally designed to control access, facilitate policing, minimize loitering, and smooth the flow of shopping. Toward such ends, malls could utilize PerC to profile their would-be inhabitants. At the border, this profile could be used to limit or discourage entry into the mall or into some subspace, such as an upscale jewelry store.[86] Postentry, the profile could be exploited to encourage mall inhabitants into a passive, consumption-only mindset.

1. Enclosing

Consider first how PerC could constrain entry, thereby undermining the ideal of accessibility of the public sphere. Of course, accessibility can be limited through strategies predating PerC, such as siting a mall away from public transportation[87] or restricting hours of operation. Still, PerC provides an additional, more sophisticated and granular layer of access control.

Generally, PerC helps the mall identify "undesirables" by examining individuals' immediate attributes for disliked characteristics. A person might fall into a pariah category because of what she is wearing, who she is "hanging out" with, or her demographic category. For example, if a mall wants to enforce a dress code, RFID scanners could read clothing types at mall entryways, elevators, and escalators.[88] A person without a recognized shirt tag might become what Marc Smith calls an "object of interest"[89] for local security guards bent on enforcing a "no shirts, no service" policy.[90] Just as easily, the

85. For a description of some of that science from the perspective of A. Alfred Taubman, see generally Malcolm Gladwell, *The Terrazzo Jungle*, NEW YORKER, Mar. 15, 2004, at 120, 122–24.

86. *See, e.g.*, *The Jeweler's Dilemma*, NEW REPUBLIC, Nov. 10, 1986, at 18 (posing ethical and legal questions related to buzzer entry systems in jewelry stores, which can be disparately deployed against young African American men).

87. Other factors include marketing, the mix of stores contained by the mall, and the availability of goods and services attractive to a particular category of consumers.

88. One could retort that visual inspection by a minimum-wage security guard would be more cost-effective. And in most cases, this may be true. But it is easy for people to take shirts off after making it past a guarded entryway.

89. The authors thank Marc Smith, a sociologist at Microsoft Research, for introducing this concept in this context.

90. The same goes with low-brow store requirements simply for "shoes" and high-brow

readers can scan for pocketknives, spray-paint, or guns. As another example, consider a mall's concern with youth gangs. Infrared sensors, which can distinguish warm-blooded human beings from their environments, can be paired with RFID readers or other radio sensors. If the same infrared+radio beacon "object" moves persistently with many other objects, then they can be automatically recognized as a "group." A group of four might be presumed to be a family; a group of seven, however, might become an "object of interest" that triggers direct video surveillance by a human security guard and a visit by "mall assistants."

An individual could also be discouraged from entry because her identity is linked to recent context trails, such as a visit to the gun store or negative reputation in a permanent financial, criminal, marketing, or other "blacklist"[91] database. Consider, for example, the facts of *State v. Wicklund*,[92] one of the many mall "public forum" cases that examined whether state law provided a right of access to private property for expressive purposes.[93] In *Wicklund*, the Minnesota Supreme Court held that state constitutional provisions went no further than the federal First Amendment;[94] accordingly, the protesters had no constitutional right of access to the Mall of America.[95] What is more relevant to our discussion is the fact that those seeking access were fur protesters.[96] If

---

requirements for "jacket and tie."

91. Consider, for instance, a blacklist of "troublemakers" shared by mall proprietors.

92. State v. Wicklund, 589 N.W.2d 793 (Minn. 1999).

93. Private property owners are generally allowed to exclude and prohibit speech on their own property. The federal constitutional right to freedom of speech does not apply to them because they are "private actors" to whom the First Amendment does not apply. Hudgens v. NLRB, 424 U.S. 507, 520–21 (1976); Lloyd Corp. v. Tanner, 407 U.S. 551, 570 (1972). However, the Supreme Court has ruled that states may interpret their constitutions' free speech and petition provisions more broadly than that of the federal Constitution. Pruneyard Shopping Center v. Robins, 447 U.S. 74, 81 (1979). This is precisely what some states have done, thereby barring shopping centers from prohibiting speech entirely and instead only permitting reasonable and generally content-neutral speech burdens. *See, e.g.*, Robins v. Pruneyard Shopping Center, 23 Cal. 3d 899, 910 (1979), *aff'd*, 447 U.S. 74 (1979) (holding that the California Constitution's free speech and petition provisions protect the reasonable exercise of speech and petitioning in privately-owned shopping centers). For a comprehensive listing of which states have gone which way, see Harriet Dinegar Milks, Annotation, *Validity, Under State Constitutions, of Private Shopping Center's Prohibition or Regulation of Political, Social, or Religious Expression or Activity*, 52 A.L.R. 5th 195 (1997).

94. State v. Wicklund, 589 N.W.2d 793, 803 (Minn. 1999).

95. This 4.2 million square foot mall, located in Bloomington, Minnesota, is the largest shopping mall in the United States. Annually, it attracts 37.5 million visitors. Coffin, *supra* note 77, at 634 (citing Brief for Appellants at 7, State v. Wicklund, 589 N.W.2d 793 (Minn. 1999) (No. C7-97-1381)).

96. *Wicklund*, 589 N.W.2d at 795.

they could, mall operators would surely maintain an electronic list of such "rabble-rousers."

This form of access control, which requires indexing individuals to their reputations, requires authenticating identity. That has never been a trivial task. But consider how convenience and security fears might prompt us to disclose our identity not only when we make a credit card purchase but simply when we enter a mall. Imagine two options: (1) wading through a long security line for those *without* the smart / credit / RFID-enabled / frequent-shopper / frequent-traveler / get-your-free-"miles" / e-discount / "celebrate your preferences"[97] lifestyle card, and (2) zipping right into nearly any mall by waving your wallet or purse past a RFID reader. Which would you choose?[98] Many of us, if not most, will "volunteer" to be authenticated just as we do when we pay with a credit card and not with cash. And interestingly, those of us who choose to maintain anonymity, simply by expressing this preference, may become "objects of interest."

We should not exaggerate the degree of enclosure; social norms will probably prevent outright exclusion of the poor or credit-challenged, except in the most elite shopping spaces.[99] But reframed in security terms, the exclusion of those with any brush with law enforcement,[100] mental illness, or civil

---

97. This phrase comes from a remarkable short story by George Saunders that captures the feeling of a nightmarish fusion of pervasive computing and consumerism. *See* George Saunders, *My Flamboyant Grandson*, NEW YORKER, Jan. 28, 2002, at 78, 81 (describing the intrusion of a "Citizen Helper" who notices that the main character's shoes' embedded tags are no longer being read by the sidewalk and is concerned about the loss of a "significant opportunity to Celebrate [the main character's] Preferences").

98. Steven Brill, the creator of Court TV, recently launched a company to provide ID cards that would enable customers to bypass security checks by verifying that they are not on terrorism watch lists and do not have certain felonies on their records. John Schwartz, *Venture to Offer ID Card for Use at Security Checks*, N.Y. TIMES, Oct. 23, 2003, at C4.

99. *See, e.g.*, Bruce Mohl, *On Ban, Basement's Mostly Mum*, BOSTON GLOBE, July 16, 2003, at C1 (describing the "barrage of media coverage" that followed a decision by Filene's Basement to ban two customers from the store due to excessive returns and complaints), *available at* 2003 WL 3408357.

100. The National Crime Information Center database, an FBI database with over thirty-nine million criminal records, was recently exempted from the accuracy requirements of the Privacy Act of 1974. Privacy Act of 1974; Implementation, 68 Fed. Reg. 14140 (Mar. 24, 2003) (codified in 28 C.F.R. § 1696(k)(4) (2004)). The FBI determined that maintaining the records with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individuals would interfere with law enforcement functions. For an opposing view, see Coalition Letter to the Office of Management and Budget Requiring Accuracy for the National Crime Information Center (NCIC) System, *at* http://www.aclu.org/CriminalJustice/CriminalJustice.cfm?ID=12306&c=15#_ftn1 (Apr. 8, 2003) (urging the Office of Management and Budget to review and revise the rule) (on file with the Washington and Lee Law Review).

disturbance could be seen as socially reasonable. Moreover, we ought to appreciate subtler tactics. For instance, when shoppers enter a store, they could immediately be classified based on wealth, credit, and individual purchase history. Salespeople would then focus on lucrative customers. By contrast, window shoppers would be politely ignored.[101]

One final novelty in this discussion warrants mention. Enacted environments raise the possibility of autonomous enclosures that respond to preprogrammed rules, largely shielded from local human discretion. A banal example is the guarded door to the airline lounge, available only for extremely frequent travelers, as authenticated by a frequent-flyer card. A more interesting example would be the buzzer to the jewelry store's door. Just as the local 7-11 advertises to would-be robbers that the safe cannot be opened by the clerk, could a sign in front of an upscale jeweler state that access is predetermined by management's "code" and cannot be overridden by the sales clerk, except in emergencies? In such cases, to whom might an indignant, rejected would-be shopper complain?[102]

We have so far identified only costs to accessibility. But, to be fair, there could be countervailing benefits: Even if accessibility is decreased for some, accessibility may be increased for others who are now scared away from public spaces. On balance, the objection goes, there could be a net gain of access—an empirical question. As discussed below, we recognize the importance of a minimum degree of safety and, more important, the perception of that safety to maintaining the public sphere.[103] But we must be thoughtful about the tradeoffs.

In particular, encouraging access to the mall by removing strange and disconcerting elements undermines a principal function of the public sphere. Such exposure is part of the public sphere's very essence. And the descriptively accurate claim that some people are put off by the odd is not an answer to the social psychological observation that repeated exposure to the "odd" makes the "odd" less odd. It is also no answer to the normative claim

---

101. Some companies, including Fidelity Investments, have begun using differentiated customer service to encourage unprofitable customers to take their business elsewhere. At Fidelity Investments, if a customer calls customer service too often, he or she will be placed on hold much longer than other customers. That customer will presumably then either stop calling or move to a competitor. Larry Selden & Geoffrey Colvin, *Will This Customer Sink Your Stock?; Here's the Newest Way to Grab Competitive Advantage: Figure Out How Profitable Your Customers Really Are*, FORTUNE, Sept. 30, 2002, at 128.

102. This raises difficult questions about whether it is better to let such decisions be made by humans, usually on a hunch, or by code, on a more formally articulated rule.

103. *See infra* Part IV.B.2 (discussing concerns about safety).

that such cultural inoculation is an important virtue, that these very perturbations mature us into citizens.

2. Flattening

In addition to enclosing, PerC can make the commercial imperatives of the mall so compelling and total as to flatten out *multiple uses* of that space. As explained above,[104] PerC brings some of the digital information economics of cyberspace into real space. This makes possible in real space the database marketing tactics perfected in cyberspace. The database marketing approach tries to collect as much information as possible about potential customers to target them with specific products, services, and advertisements. The Internet has transformed this practice by making information collection far cheaper than ever before. Through the use of various tracking technologies, such as cookies, advertisement banners, spyware, and site registration, individuals' browsing patterns are being collected and analyzed for commercial opportunity.

PerC allows the information economics that exist today in cyberspace to cross into real space. The ease of gathering personal data during online browsing will spillover into real space window-shopping.[105] Imagine if every brick-and-mortar store adopted Amazon.com practices, including its automatic user registration through an RFID super-shopper-mall pass; comprehensive record of past purchases as well as window-shopping, not only at that store but all other affiliates; and automatic recommendations of complementary items to purchase. This scenario highlights how augmented reality can be experienced not only by individuals but by the corporation. And through its datasense, the firm lays a data profile over us as targets of commercial opportunity.

In designing its enacted environment, the store could manipulate the data flows we receive—unique offers, prices, and discounts—as well as alter the environment we experience to make the sale. More radical examples could

---

104. *See supra* Part II.B.2 (discussing ways in which computing will pervade the real world).

105. Consider, for example, one potential application of RFID technologies to decrease theft of razor blades. The UK supermarket chain Tesco has tested the use of RFID tags embedded in Gillette-brand razor blades to trigger a closed-circuit TV picture when the razors are taken off the shelf and another picture at the point of sale. Alok Jha, *Tesco Tests Spy Chip Technology*, THE GUARDIAN, July 19, 2003, at 10, *available at* 2003 WL 56698830. The cameras may have been employed just to test the functioning of the RFID systems, not as a preview of some elaborate antitheft system Tesco intended to implement. *Id.* Still, even if Tesco and Gillette were not interested in such an implementation, others will surely be.

include altering micro-climates that change the music and colors experienced in any nook of the store, which may be personalized to a specific individual or to the average profile of the group occupying the same region.[106] In fact, through its sensors, the store could detect types of information unavailable today. Your low body heat or repeated sniffles might trigger a "pop-up" advertisement for a warm hat bundled with free tissues.[107] Your sudden uptick near lingerie might suggest a rated R feature at the gigaplex. We will not be able to resist.[108]

The infrastructure that generates perfectly tailored offers implies continuous surveillance within the mall—not for security but commerce. This surveillance will benefit from PerC's deep invisibility, which obscures what we are, in fact, sharing in the public's eye. Moreover, the invisible distribution of data means that we cannot presume to know what others see and hear. Is everyone receiving the same toaster oven ad, or is this special offer just for me? Is everyone being charged the same price for this item, or am I the object of perfect price discrimination?[109] This veiled sub- and

---

106. *See* Saunders, *supra* note 97, at 78, 80 (imagining "Kakio Aural Focussers" which target sound-only messages to specific individuals and "Cybec Emergent Screens" that thrust targeted holographic advertisements into view).

107. For a slightly dated review of what advertising might look like in the wireless space, see FTC, *supra* note 26, at 677–79.

108. One might object that there is nothing wrong with satisfying people's preferences. Indeed, most law-and-economics practitioners take individual preferences as exogenous and their satisfaction to be the principal goal of society. However, the public sphere is supposed to reshape individual preferences. And a public space that becomes exceedingly good (although not perfect) at creating desires for consumer goods, then satisfying them, becomes less of a space for other purposes. We discuss this matter further as we flesh out the idea of "friction mall."

109. Price discrimination means charging different buyers different prices even though the cost of providing the good or service is indistinguishable. *See* WILLIAM W. FISHER III, PROMISES TO KEEP: TECHNOLOGY, LAW, AND THE FUTURE OF ENTERTAINMENT 163–69 (2004) (discussing price discrimination in the context of a potential intellectual property regime as robust as our current real property regime). First-degree price discrimination takes place when sellers have perfect information about what each buyer is willing and able to pay, and sets the price accordingly. *Id.* at 165. Second-degree price discrimination takes place when sellers, who lack such information, elicit it in the marketplace by offering multiple options set at very different prices even though they are minor variations on the same product. *Id.* Third-degree price discrimination is a realistic implementation of the first-degree variety when perfect information is unavailable. *Id.* It entails profiling potential customers into different categories, for example on the basis of financial reputation and previous purchase history, then charging those categories different prices. PerC has the ability to facilitate substantially this third type of price discrimination.

Calculating the social costs and benefits of third-degree price discrimination abetted by PerC is difficult and beyond the scope of this paper. One should not jump to the conclusion, however, that it will necessarily produce more progressive pricing, with higher prices for the

superstructural operation raises uncertainty about what we know, what is known, and what is shared.

Such Panopticon-like surveillance may chill speech and behavior—not only the illegal but also the marginal and irregular.[110] 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?[111] The fact that you are surveilled by private firms for "marketing" purposes and not by the state for national security purposes means little when the state can easily buy or subpoena private data.[112]

In sum, through positive reinforcement of consumerism and negative reinforcement of "irregular" behavior, PerC can further flatten public sphere qualities of the shopping mall. By sensing not only your physical body but also your data profile, the enacted environment of the mall will be able to invite you—should you qualify—into a brave new hyper-commercialized world where your role as consumer will dominate, and happily so. By threatening to know so much more about you, PerC will also chill irregular, deviant, or unpopular speech and actions. In turn, this homogenization of speech and behavior will feed back into our social norms, thoughts, and (lack of) imagination. For some, this chilling is precisely what we need more of, to build a more civil society, which encourages safe interaction among citizens.

---

wealthy and lower prices for the poor. This would depend on various variables including market power and demand elasticity. For instance, if the poor have inelastic demand and fewer competitive options, they may have to pay more, not less. For a highly critical view of price discrimination in information markets, see generally Julie E. Cohen, *Copyright and the Perfect Curve*, 53 VAND. L. REV. 1799 (2000).

110. Kang, *supra* note 31, at 1260–61.

111. *See, e.g.*, David Johnston, *Somali Is Accused of Planning a Terror Attack at a Shopping Center in Ohio*, N.Y. TIMES, June 15, 2004, at A16 (discussing the prosecution of an alleged Al Qaeda affiliate for planning to bomb a Columbus mall).

112. The Total Information Awareness (TIA) program was designed to mine data in commercial as well as government databases to spot patterns that could indicate terrorist activity. Hiawatha Bray, *Mining Data to Fight Terror Stirs Privacy Fears*, BOSTON GLOBE, Apr. 3, 2003, at C2, *available at* 2003 WL 3388980. Although Congress eliminated funding for TIA, similar efforts continue. *See* Duane D. Stanford, *ACLU Attacks Matrix on Privacy*, ATLANTA J.-CONST., Oct. 31, 2003, at 3G (describing an initiative by several state governments to develop a program similar to TIA, the Multistate Anti-Terrorism Information Exchange (Matrix)), *available at* 2003 WL 66525863.

Our concern is that we will give up more than we bargain for. Renouncing the unfamiliar, we will simply commingle with fellow slaves-to-fashion.[113]

B. Friction Mall

Imagine a different future that does not relinquish to the mall plenary power over the informational environment. Instead of hierarchical domination, imagine open, decentralized, peer-to-peer interactions. Instead of passive TV consumption, the model is the Internet.[114] Anarchy, information overload, and interference are all possibilities, and yet so is proliferation of the public sphere.

1. Political Shopping

Imagine a person buying a coffeemaker. She scans it with her communicator, which identifies the electronic product code, then provides a flurry of counter-information: an environmental group reminds her of coffee production's role in deforestation; the store on the next level offers the same item at a cheaper price; a competing manufacturer sends an advertisement for its brand bundled with an electronic "free latte" coupon immediately redeemable at the Starbuck's three stores down. Or, suppose that the enacted environment lights up, literally, a path for the shopper to follow toward an attractive winter jacket. But just in time, her augmented reality notes the manufacturer's use of sweatshop labor and how the flame-retardant chemical in the fabric has been banned everywhere except the United States.[115] Given this overlay, she decides that the jacket has to be discounted at least another ten percent before she buys it. Or finally, imagine a diner hearing a tempting

---

113. Julie Cohen raises similar fears of flattening in a recent paper examining how digital rights management technologies implemented in a context of "crisis discipline" threatens to produce "standardized, homogenized space." Julie E. Cohen, Normal Discipline in the Age of Crisis 39 (July 2004) (unpublished manuscript, on file with the Washington and Lee Law Review).

114. *See, e.g.*, Yochai Benkler, *From Consumers to Users: Shifting the Deeper Structures of Regulation Towards Sustainable Commons and User Access*, 52 FED. COMM. L.J. 561, 575 (2000) (decrying the production of a consumer-mindset on every layer—content, logical, and physical—of our communications environment).

115. The European Union has banned certain types of PBDEs, a common flame retardant chemical linked to numerous health problems, while the EPA continues to evaluate the chemical. Jane Kay, *Study Finds Flame-Retardant Chemical in U.S. Breast Milk*, S.F. CHRON., Sept. 23, 2003, at A4, *available at* 2003 WL 3763582.

special about "swordfish" at a restaurant only to have her communicator recognize that speech, recognize the fact that she is at a restaurant during meal time, and then vibrate a health alarm about the FDA's warnings about mercury pollution. She declines the expensive special to the waiter's annoyance.

As these examples suggest, an open information environment can reveal what seemed like the Siren call to be the huckster's pitch. If PerC can deliver such tailored information in real-time, then our shopping decisions can be based upon multiple sources, such as Consumer Reports as well as political organizations engaged in boycotts of retailers and manufacturers for labor, environmental, and other political reasons.[116] Of course, the counter information should not overwhelm or spam us; rather, the information should be highly context-sensitive so as to be timely, relevant, and chosen to be received.

Indeed, operating within these constraints, a whole new range of sociopolitical intermediaries could help facilitate "political shopping" by providing not only information about quality and price, but also social, environmental, and justice consequences.[117] Before ordering veal parmigiana, Paul McCartney might sing in one's ear about animal cruelty. Before buying an overpriced shirt at Abercrombie & Fitch, the National Asian Pacific American Legal Consortium might provide a reminder about the firm's sorry history with racial minorities.[118] Choosing among three fungible gas stations at a nearby corner, one might rely on the Sierra Club's recommendation.

Political shopping is not the Greek agora, the romantic pinnacle of politics in the public sphere. Still, it helps resist the flattening of uses of mall space. The very act of shopping becomes entangled with other activities and

---

116. *See* Jonathon D. Glater, *The Ultimate Bar Code: Imagine the Possibilities*, N.Y. TIMES, Sept. 7, 2003, at WK2 (describing an invention that scans bar codes and makes a noise if the manufacturer is the subject of ethical complaints); *cf.* Invertix Corp., *supra* note 27 (describing the mNET Campaign Results Tool, which allows wireless instant messaging of advertisements and coupons to subscribers based on geolocation and preference settings).

117. *Cf.* Jerry Kang, *E-racing E-lections*, 34 LOY. L.A. L. REV. 1155, 1167–68 (2001) (discussing the potential rise of voting intermediaries with electronic voting systems).

118. Nine Asian Americans and Latinos sued Abercrombie & Fitch for employment discrimination. Elizabeth Kelly, *Claims Against Abercrombie Detailed; Nine Students Say They Were Fired or Not Hired Because They Didn't Fit the 'A&F Look'*, L.A. TIMES, June 18, 2003, at C2, *available at* 2003 WL 2413260. A year earlier, the chain began selling T-shirts with caricatures of Asians as laundry owners and rickshaw drivers. The shirts were quickly pulled off the shelves due to complaints that they promoted racial stereotypes. *See* Gina Kim, *Racism Doesn't Belong on T-Shirts, Crowd Tells Abercrombie & Fitch*, SEATTLE TIMES, Apr. 28, 2002, *available at* 2002 WL 20270334; *cf.* Yick Wo v. Hopkins, 118 U.S. 356, 374 (1886) (holding that San Francisco's discriminatory application of regulations regarding public laundries violated the Fourteenth Amendment).

purposes, politics, and normative commitments. In this way, PerC could help subvert the dominant ideology of what a shopping mall molds its inhabitants to be. Instead of the largely passive shopper, consuming store windows like television channels and acquiring commodities to satisfy advertisement-induced lifestyle desires, we could help construct the "activist shopper," who is more self-critical, indeed ironic, in maximizing complex, marbled, and overlapping sets of interests.

The above examples of political shopping emphasize how augmented reality could provide relevant information, in real-time, to counter the enacted environment's perfectly profiled offer. The relevant information need not come from some centralized source or intermediary, such as Consumer Reports or the ACLU, much less the Federal Trade Commission. Instead, it can take full advantage of peer-to-peer networks localized at the specific shopping site. If the food was awful and the service rude, we could spatially annotate[119] the restaurant with our comments. Potential diners could search for such information, filtering that data by relevance, recency, and reputation of source.[120] The same could go for other sorts of stores and services offered at the mall. The collective experience, knowledge, and judgments of shopgoers could help create long-term reputations for stores, accessible even to those just passing through.

2. Meeting Strangers

In addition to the manifest function of a shopping mall—namely shopping—the mall serves myriad latent functions, ranging from adolescent socializing to senior citizen physical exercise. As any urban teenager can testify, the mall is a prime site for dating, hanging out, and meeting new friends. How might PerC facilitate such practices that, although connected to shopping and consumption, are different and add another layer of use to the mall? More specifically, how might PerC facilitate social exchanges between strangers, who by virtue of race, age, clothing, or appearance, would not have otherwise interacted? After all, these are foundational goals of the public sphere. These questions require us to explore what keeps mutually interesting

---

119. *See* Marc A. Smith, *Some Social Implications of Ubiquitous Wireless Networks*, 4 MOBILE COMPUTING & COMM. REV. 25, 27 (2000) (discussing the work of the MIT Media Lab's Tangible Bits Group).

120. We should, as always, be cautious about the source and quality of information, including those generated in peer-to-peer contexts. Self-interested parties spoof identity to post glowing reviews of their products as if they were disinterested consumers; Amazon has had to address "prank mobs"; Google has had to resist Google-hacking.

co-present people from interacting.[121] Two factors stand out: (1) lack of information about who is mutually interesting and (2) concern about safety.

Ignorance. Consider how PerC could alleviate the first problem by matching people who would find each other interesting because they know the same people or share similar goals, interests, and experiences. Internet dating convincingly demonstrates that information technologies can drastically lower the transaction costs of meeting mutually interesting people. The same will be so with PerC, but with greater spontaneity within specific localized geographies.[122] Some of this may have to do with dating. Social exchanges could also be catalyzed on the basis of those shared interests, fates, and experiences that create virtual communities online:[123] a love for cats, an expertise in rare coins, surviving cancer. Recent software developments turn network users into homing beacons who, finding themselves in proximity, can scope each other's publicly posted profiles to see if they want to chat electronically or get together physically.[124]

The programming of mutual interest filters raises significant questions not only about privacy but also about the vocabulary and grammar of expressing preferences. These questions have already extensively been explored in the context of the television V-Chip, the Platform for Internet Content Selection (PICS),[125] and the Platform for Privacy Preferences (P3P).[126] Another danger

---

121. We recognize that social interaction is not always desirable. Regardless of how many items of interest in common with someone waiting in line for a coffee, one may seek silence, not conversation. In this discussion, we are focusing on the cases in which people would like to engage socially but do not know quite how to start.

122. The most substantial implementation of this technology is the Lovegety in Japan. *See Lookin' for Love in New Cyber Spaces*, *at* http://www.geocities.com/Pentagon/Bunker/5921/lovegety.html (last visited Oct. 16, 2004) (describing the Lovegety device) (on file with the Washington and Lee Law Review). For a proposed rollout in the United States, see Invertix Corp., *supra* note 27 (describing mNET Dating, which notifies users whenever matches are found nearby).

123. *See* Kang, *supra* note 78, at 1164 (discussing ways in which technology can bring people together).

124. A firm called Trepia once produced a software program that allows individuals to locate other users that are geographically nearby, review their profiles, and contact them. *See* Paul Boutin, *Putting the World Into the Web*, SLATE, *at* http://www. slate.msn.com (May 30, 2003) (discussing the uses of Trepia) (on file with the Washington and Lee Law Review). Even if they are using separate neighboring networks, they can become aware of each other. *See* Spotme Brochure, *supra* note 44 (discussing the features of Spotme).

125. JERRY KANG, COMMUNICATIONS LAW & POLICY 278–80 (2001).

126. World Wide Web Consortium, *Platform for Privacy Preferences (P3) Project*, *at* http://www.w3.org/P3P (last visited Oct. 29, 2004) (on file with the Washington and Lee Law Review).

is cocooning: We will choose to meet only the like-minded and the similar.[127] Even if there is a "physical" world diversity, our filters may create a "logical" world homogeneity by dropping people or groups out of our attention network.

Which result PerC produces depends on design and implementation. Stated abstractly, the trick is to encourage exchange based on certain factors that cut across traditional cocoon-categories. We often make decisions about whom we want to meet on the crudest outward appearances. But certain shared items, revealed through our augmented realities, can make more complex the factors that draw our attention. The fact that two people have read the same book recently, for example, can be a crucial conversation catalyst. And those two people may have very different fashion senses, which might have otherwise precluded any initial exchange. A design decision—not by the state, but by private sector technologists—could hinder or enhance our ability to express preferences for social engagement to nontrivial impact.[128]

Fear. The other factor that keeps us apart, besides ignorance, is fear for safety. Might PerC soften our fear of strangers by helping to establish trust? Trust and risk, according to sociologist Anthony Giddens, along with security and danger, are central concepts to an understanding of contemporary life.[129] The perceived danger of public urban space has contributed to its demise. Here we again acknowledge that one potential benefit of what critics call chilling surveillance, facilitated by PerC, is comforting security. And in such a climate, people might let their hair down and engage with those around them,

---

127. Many commentators have worried about how the Internet allows for excessive personalization of information flows. In other words, if we are interested only in a particular topic, then we can construct filters and instruct software agents to deliver us only that sort of information. This excessive "cocooning" effect can undermine the cache of public, shared experiences and knowledge necessary to maintain a deliberative democracy. *See generally* CASS SUNSTEIN, REPUBLIC.COM (2001). *But cf.* Anupam Chander, *Whose Republic?*, 69 U. CHI. L. REV. 1479, 1488 (2002) (book review) (questioning whether the pre-Internet general interest intermediaries are essentially assimilationist, not multicultural). *See generally* Eugene Volokh, *Cheap Speech and What It Will Do*, 104 YALE L.J. 1805 (1995) (arguing that the Internet would reduce the cost of distributing speech, thereby making democratic, diverse speech more widely available).

128. Many colleges have begun matching incoming freshmen with roommates using personal information such as study habits and sleeping schedules, but race is not considered. *See* Tamar Lewin, *First Test for Freshmen: Picking Roommates*, N.Y. TIMES, Aug. 7, 2003, at A1 (describing the roommate matching systems at Emory and Barnard; Barnard occasionally gets requests based on race despite stating on the preferences form that race will not be considered).

129. *See generally* ANTHONY GIDDENS, THE CONSEQUENCES OF MODERNITY (1990). He identifies "globalized risks," like global warming or nuclear war, that collectively affect large numbers of individuals. *Id.* at 124–26. Acceptable risk, the minimizing of danger, is generally balanced by trust, resulting in a level of security. *Id.* at 131–34.

even those who seem different. In addition to promoting general feelings of safety, PerC could provide more individualized reassurances through real-time reputation data that would allow individuals and institutions to directly or indirectly vouch for others. If you must leave your bags unattended for a moment, you might be more inclined to ask the adolescent who is recognized as a friend of a friend of your child.[130]

It is difficult to strike the right balance between, on the one hand, a private-police state, complete security with no freedom,[131] and, on the other hand, a site perceived to be so dangerous as to be abandoned. Furthermore, given limited resources and political will, the preferred cop on the beat may not be an alternative to videocameras in the ceilings.

But if we are stuck with some bad, we should strive to reap some good. More specifically, if surveillance becomes rampant in the mall, we might as well leverage that reality to produce the safety that will free individuals to engage in a broader range of social exchanges. The objective is to avoid what many have lamented as the Disneyfication of social space,[132] in which the forms of surveillance and control become near total. What we seek are middle grounds in which trust and risk are balanced, with one never totally vanquishing the other.[133] This new middle ground sits between two extremes, the perceived-dangerous street that many have abandoned and the complete safety of cyberspace shopping. Easier said than done.

V. Design Principles

---

130. The website www.friendster.com enables users to meet or date people to whom they are connected through mutual friends. Rodney Ho, *Site Too Friendly for Its Own Good*, CONTRA COSTA TIMES, Nov. 12, 2003, *available at* 2003 WL 75791662. Users set up a profile page, and then link to their friends' pages. *Id.* They can then access and search the profiles of friends of friends of friends, out to four degrees of separation. *Id.* The website calculates the number of people to whom you are connected, and the networks quickly grow very large; for example, one person has 187 "first-link" friends, and 950,000 people are within four degrees of separation. *Id.*

131. For science fiction articulations of such a future, see, for example, LARRY NIVEN & JERRY POURNELLE, OATH OF FEALTY (1981) (describing an enclosed mall-city in the near future of Los Angeles that is totally surveilled, totally safe, and whose access is totally regulated).

132. *See* Barber, *supra* note 76, at 206 (describing Disney's amusement parks and its city, Celebration, Florida). Barber writes that through Disney, "[w]e are inoculated against infection by the truly different with an immunizing shot of the superficially distinctive." *Id*. at 209.

133. One approach we tentatively propose would be to ensure against catastrophic dangers without denying access to the mall. At access points, the mall could screen for weapons. And everyone could have GPS-enabled panic buttons, perhaps activated on their mobile phones or on frequent shopper pagers. This program would go a long way to create the perception of safety that might rejuvenate certain public spheres.

Above, we painted two stylized, divergent portraits of the percolated mall. Which future will come to pass? Given the current array of forces undermining the public sphere, we are pessimistic unless specific interventions embed the "public sphere" into PerC as PerC simultaneously embeds itself into the public sphere. Which interventions are appropriate will always depend on the specific context. Our goal here is to tease out broad design principles to inform subsequent, more particular discussions.

A. Privacy

Obviously, much of our discussion raises central questions about information privacy, defined as an individual's claim to control the collection, disclosure, and processing of personal information.[134] How we answer these questions, by resetting the balance between privacy and publicity, fundamentally shapes the public sphere. When individual privacy is eroded through surveillance technologies or data collection, our public domain is implicated. On the one hand, people might avoid totally surveilled spaces, especially if collected information is misused.[135] On the other hand, we recognize that some surveillance can promote senses of safety, which could revivify certain public spaces.

For reasons argued elsewhere, we believe that personal information generated by PerC technologies in the course of any shopping interaction should be legally treated according to a default rule of "functionally necessary use."[136] In other words, federal statutory law should require that personal data

---

134. *See, e.g.*, Kang, *supra* note 31, at 1205 (explaining that this is the standard definition used in the literature).

135. Consider, for instance, how the Department of Homeland Security's resources were deployed to track down Texas Democrats dodging a quorum. R. Jeffrey Smith, *In Texas Feud, a Plane Tale of Intrigue*, WASH. POST, June 7, 2003, at A1.

136. *See* Kang, *supra* note 31, at 1249–59 (arguing for a ground rule of "functionally necessary use"). I proposed the following language in a model statute:

> "Functionally necessary" describes personal information processing that is necessary to execute the cyberspace transaction in which the personal information is originally acquired. This is limited to information processing necessary for successful communication; payment and delivery; dispute resolution; warnings to the individual of any defect or danger; maintenance of cyberspace infrastructure; protection from fraud and abuse; adherence to governmental recordkeeping regulations; and transfer of business ownership. It expressly excludes processing of personal information to target information, services, and goods on the basis of that personal information to the individual.

Id. at 1290.

collected in the course of any such interaction may be used by the mall only to complete that interaction. Any other functionally unnecessary use, including advertising, would require separate consent from the individual. The case for this default rule, with detailed statutory specifications, was made in the context of cyberspace; however, PerC introduces similar information economics to real space. Thus, it now makes sense to apply this default rule to percolated environments outside of cyberspace as well.[137]

The case for this default rule was made not only on human dignity grounds, which invites sharp ethical and philosophical disputes, but also on economic efficiency grounds, which in current (de)regulatory circles seems to be the uncontroversial purpose of law.[138] Instead of repeating that argument here, we simply add that the technologies of PerC themselves could potentially help enable the "functionally necessary" rule or other politically agreed-upon data practices.

For example, some technologists have called for the creation of privacy "faces," which could be emitted by wearable computing that represent a summary of consent to certain types of data processing activities.[139] Another example is information architecture and grammar that allows privacy attributes to "stick" to the personal data as it flows through multiple information spaces.[140] More generally, if, as Gary T. Marx argues, reasonable expectations of privacy are often violated when certain traditional social, spatial, or

---

137. Our favoring a default rule of "functionally necessary use" may obstruct the smooth mall vision. Such a legal entitlement certainly provides greater privacy protections than exist today. That said, we do not believe that it would necessarily prevent the smooth mall approach from being implemented. It may turn out that even after reasonably clear notice, individuals will generally consent to functionally unnecessary uses to reap the benefits of discounts and customization. This possibility shows some of the limitations of the individual consent-based model of privacy protections. *See generally* Jerry Kang & Benedikt Buchner, Privacy in Atlantis (Nov. 29, 2004) (discussing significant policy ramifications inevitably flowing from such a definition of privacy) (unpublished manuscript, on file with the Washington and Lee Law Review).

138. Whether privacy discourse sounding in human dignity or economic efficiency is all that different, in practice, is another question. *See generally id.* (exploring this theme in the form of a Socratic dialogue).

139. *See, e.g.*, SCOTT LEDERER ET AL., EVERYDAY PRACTICE IN UBIQUITOUS COMPUTING ENVIRONMENTS § 3.3, *at* http://guir.berkeley.edu/pubs/ubicomp2002/privacyworkshop/papers/lederer-ubicomp02-workshop.pdf (last visited Nov. 16, 2004) (discussing a use of privacy faces) (on file with the Washington and Lee Law Review). Whether this provides any more on-the-ground experience of privacy than say, P3P, is an open question.

140. IBM's Enterprise Privacy Authorization Language is described in this way. *IBM Submits EPAL Version L2 Privacy Specification to W3C*, *at* http://xml.coverpages.org/ni2003-12-04-a.html (Dec. 4, 2003) (on file with the Washington and Lee Law Review).

temporal "boundaries" are crossed by data processing,[141] then PerC technologies could help detect where those boundaries lie. These boundaries can be physical, defined by geolocation,[142] or understood more abstractly, as social or activity-based.[143]

We press on to discuss other design principles that are related to, but interestingly different from, the salient issue of information privacy.[144] Again, we seek to be suggestive and explorative, not comprehensive.

B. Transparency

One way to increase accountability regarding mall surveillance is to increase the transparency of how that otherwise invisible surveillance is conducted.[145] For instance, if people are denied access at the mall's entry, they should have legally enforceable access to the reasons for their denial with reasonable rights of correction. An obvious analogue is the Fair Credit Reporting Act.[146] If individuals are being put into second class shopper status,

---

141. GARY T. MARX, UNDERCOVER: POLICE SURVEILLANCE IN AMERICA 223 (1988).

142. An ingenious application of this general idea in the RFID space comes from Kenneth Fishkin and Sumit Roy. They point out that "distance" between the reader and the RFID implies "distrust." Since this distance can be estimated by the amount of energy the RFID tag receives and some signal-to-noise calculations, the additional variable of "distance" could be used to determine how much a tag should trust the RFID reader that requests information. Another obvious variable to consider in the trust assessment is, for example, whether the RFID reader possesses the correct cryptographic key. The greater the trust, the more information that could be released. *See generally* Kenneth P. Fishkin & Sumit Roy, *Enhancing RFID Privacy Via Antenna Energy Analysis*, RFID Privacy Workshop, Nov. 15, 2003, *available at* http://www.rfidprivacy.org/2003/papers/fishkin.pdf.

143. *See, e.g.*, Xiaodong Jiang & James A. Landay, *Modeling Privacy Controlling Context-Aware Systems*, PERVASIVE COMPUTING, July–Sept. 2002, at 59, 61 ("[M]any context-aware technologies exist precisely to identify such borders in our daily life (for example, location tracking to identify natural borders). By formally capturing borders using the boundary abstraction, our information space model provides the basis for leveraging existing context-aware technologies to minimize undesirable border crossings.").

144. *Cf.* Katyal, *supra* note 3, at 1129–30 (discussing the ways in which promoting the use of public spaces through architectural design can bolster individual privacy).

145. For the most aggressive argument for transparency, see generally DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998).

146. The Act was codified at 15 U.S.C. §§ 1681–1681u (2000). The most relevant provisions appear in 15 U.S.C. § 1681g (2000) (addressing disclosures to consumers). *See* 15 U.S.C. § 1681e(c) (2000) (permitting any user of a credit report to reveal its contents to a consumer when adverse action against the consumer has been taken on the basis of the report).

they should have access rights to the information and calculation that produced that categorization.

Also, throughout the mall, the deep invisibility of PerC technology can be countered by notice requirements to counteract the mismatch between the reality of surveillance and the apparent lack of surveillance. In other words, mall inhabitants should be able to learn whether and in what ways they are being observed.

Such transparency would have two benefits. First, it would force information about the surveillance that we face daily into the light of the public sphere. Such knowledge not only allows us to make better decisions about which malls we wish to patronize, but also provides the information necessary to spark public conversations about privately adopted technologies. Second, this information would reduce the Panopticon effect. In the Panopticon, prisoners never knew whether a centrally situated guard was actually watching them. The same was true for George Orwell's 1984 two-way telescreens in everyone's home.[147] The uncertainty of surveillance fostered a climate of conformity. A transparency requirement would decrease this uncertainty and its impact.

We can imagine simple implementations of transparency, such as a downloadable database of the GPS locations of all video cameras in the mall and the regions they cover. Antisurveillance activists have posted this sort of data online, in primitive form.[148] A more sophisticated implementation would involve some real-time, color-coded representation of the surveillance environment on our augmented reality interfaces.[149] These transparency requirements could be required by law,[150] as well as adopted as critical

---

147. *See* GEORGE ORWELL, 1984, at 4 (1949) (discussing the use of two-way telescreens).

148. *See, e.g.*, *Maps of Publicly Installed Surveillance Cameras in New York City*, http://www.notbored.org/scp-maps.html (last visited Oct. 20, 2004) (showing the diagram of New York City cameras by Surveillance Camera Players) (on file with the Washington and Lee Law Review).

149. *See, e.g.*, David H. Nguyen & Elizabeth D. Mynatt, *Privacy Mirrors: Understanding and Shaping Socio-technical Ubiquitous Computing Systems* § 4.2, *at* http://erstwhile.org/~dnguyen/writings/PrivacyMirrors.pdf (last visited Nov. 16, 2004) (discussing the concept of "privacy mirrors," which could be viewed at a *glance*, involve a more substantial *look*, or be fully *interactive*) (on file with the Washington and Lee Law Review).

150. Although many states have laws designed to prevent voyeurism, those laws typically only provide protection when the subject has a reasonable expectation of privacy—meaning not in public. *See* Lance E. Rothenberg, *Re-Thinking Privacy: Peeping Toms, Video Voyeurs, and the Failure of Criminal Law to Recognize a Reasonable Expectation of Privacy in the Public Space*, 49 AM. U. L. REV. 1127, 1144–45 (2000) (stating that privacy rights do "not extend to the public space and at most serve[] only as a minimal deterrent to video voyeurism"). The only state that regulates video surveillance in public places is Arizona, which requires anyone

building practices that, for example, provide increased visibility at the control points by means of extensive use of glass or publicly projected surveillance imagery.

More interesting is the possibility of implementing a transparency norm in the PerC technology itself. What if every 3G-enabled video camera had to emit a signal that announced the fact of recording three seconds before it started? What if every RFID reader had to announce its own identity?[151] This idea is not as fantastic as it may seem. In the near future most adult inhabitants of the mall will be carrying a 3G-enabled communicator. Equipping that device with the circuitry necessary to read a few bits of information transmitted on a particular frequency, which we dub the "Orwell" frequency, would not be technologically difficult or economically expensive. Similarly, governments could easily mandate that all surveillance devices of a certain sort[152] transmit self-identifying information at that particular frequency. Naturally, the range of the transmission should be proportional to the range of surveillance. Then, whenever we were being read or recorded, our communicator could chirp and provide details about who is inquiring.

Skeptics could say that the Orwell frequency will be as useless as browser cookie notification: Constant vibration on our hips, like the constant pop-up windows telling us of cookie deposits, will prompt us to turn off the notification altogether.[153] Real space has not yet been so percolated as to produce incessant notice, but this may change. Right now a window of opportunity exists[154] for alerts induced by the Orwell frequency to provide

---

(except reporters) using video surveillance in a public place to post prominent notice. *See* Christopher Slobogin, Symposium, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 235 (2002) (stating that Arizona makes it a misdemeanor to use video surveillance in a public place without prominently posting notice of that surveillance).

151. Adding circuitry to our mobile communicators noting the existence of an RFID reader field would be trivial, as the very act of "reading" would give notice to the person being read.

152. Law enforcement could be excluded. Low resolution or fidelity devices could also be excluded. Under European law, whether a device is classified as a CCTV depends on the quality of the images captured. *See* Barry Fox, *Wireless Cameras Raise Privacy Fears*, NEW SCIENTIST, May 19, 2003, at 11 (stating that certain cell phones with digital cameras could be classified as CCTV devices), *available at* http://www.newscientist.com/news/news.jsp?id=ns99993725 (on file with the Washington and Lee Law Review).

153. *See, e.g.*, LEDERER ET AL., *supra* note 139, § 3.2 (identifying this concern and suggesting the logging of personal information collection events for ex post evaluation).

154. That window may be closing quickly. By one count, ordinary consumers are installing surveillance tools such as digital video cameras at a rate of six million dollars per day. *See* Dan Farmer & Charles C. Mann, *Surveillance Nation: Part Two*, TECH. REV., May 2003, at 46, 49 (relaying a claim by CCS, Intl., a firm that produces surveillance products).

meaningful and, at times, surprising information. As our communicators alert us more often, and in unexpected areas, we will be forced to confront the environment's percolation as a matter of public policy. By intervening now, we will not have to respond to it as a *fait accompli*, in the way that most of us might respond to the reality of cookies.

One final point bears mention. In addition to pre-observation or real-time notification, transparency can also be served through ex post discovery or its possibility. In other words, audit trails with cryptographic integrity can leave an official record of who processed what data, when, and how. What if every time a mobile telephone's radio beacon was identified or authenticated, that telephone itself would generate an audit trail of that fact? The possibility of being "seen" later can promote accountability in how surveillers surveil.[155] In closing, we recognize a cost to the transparency we advocate: Clever criminals might make use of the information, too. However, in our view, in the average mall without any special reason to fear catastrophic crime, the benefits of transparency outweigh these costs. The presumption should be in favor of transparency.

C. Open Access

Maintaining the public sphere in the shopping mall also requires open access. By "access," we do not focus here on physical accessibility, which is obviously important with or without PerC. That aspect of the term has already been discussed.[156] For instance, legal commentators have debated to what extent private mall property should be considered a "public forum" to which there is a federal or state right of access to engage in speech or petitions.[157] Instead, we focus on the ability to access information, without restriction, from local and remote sources while we occupy the private property of the shopping mall.

---

155. We observe that our recommendations regarding privacy and transparency are compatible with the "principle of minimum asymmetry" urged by Xiaodong Jiang et al., *Approximate Information Flows: Socially-Based Modeling of Privacy in Ubiquitous Computing* § 3.3, *at* http://guir.berkeley.edu/projects/ubicomp-privacy/pubs/ ubicomp2002-aif.pdf (last visited Nov. 16, 2004) (stating the principle as "[a] privacy-aware system should minimize the asymmetry of information between data owners and the data collectors and it users, by: decreasing the flow of information from data owners to data collectors and users; increasing the flow of information from data collectors and users back to data owners") (on file with the Washington and Lee Law Review).

156. *See, e.g.*, *supra* Part III.A (describing the public sphere).

157. *See, e.g.*, Berger, *supra* note 61, at 656–91 (discussing cases that address free speech rights in "market places").

The fear is that a mall, asserting private property rights, could leverage its control over physical property (the "physical layer") to control the information made available to our augmented realities (the "content layer").[158] Suppose that in the near future, local governments on public property and private actors on private property provide ubiquitous Internet access through 802.11x technologies.[159] In this scenario, the mall would provide broadband wireless Internet connections by purchasing services from some Internet Service Provider, then setting up wireless access points throughout the mall. By controlling these access points, the mall could both condition Internet access and shape its experience.

Registration and authentication are obvious preconditions to access. In addition, the mall could make information streams conducive to political shopping hard to find, slow, or entirely filtered out. For instance, Web browsing may be permitted, but not peer-to-peer applications that might be necessary for full-blown political shopping. With the limited range of 802.11x signals, shoppers inside a large mall may have no other option than to use the mall's own access points. To any complaints about censorship, the mall's response would be: "It's our property, we can do what we want." Toss in a quick reference to viruses, cyber-terrorism, or copyright infringement, and any challenge to the procedures will be deemed answered.

In sharp contrast, a common carriage implementation of ubiquitous Internet access would avoid these problems. In this scenario, an individual's access to information relies on a conduit provided by commercial mobile radio services (CMRS) providers, which are common carriers with whom the individual has a direct contractual relationship. Jamming this mobile telephony signal would constitute unlawful interference with radio signals.[160] Thus, counter-information crucial to political shopping and related social

---

158. This use of "layers" should be familiar to network engineers as well as communications theorists. *See, e.g.*, LAWRENCE LESSIG, THE FUTURE OF IDEAS 23 (2001) (describing communications systems as being made up of physical, code, and content layers); *see also* KANG, *supra* note 125, at 21–23 (describing network layers).

159. Given the delayed rollout of 3G mobile phone networks and the limited bandwidth of such systems, the widespread adoption and use of 802.11x networks is a reasonable prediction.

160. The FCC considers the jamming of wireless signals a violation of 47 U.S.C. § 333 (2000) (prohibiting interference with radio signals), and the manufacture, importation, sale, or advertising of jamming devices a violation of 47 U.S.C. § 302a(b) (2000) (restricting devices that interfere with radio reception). FCC, *Operations: Blocking & Jamming*, *at* http://wireless.fcc.gov/services/cellular/operations/blockingjamming.html (last updated Nov. 19, 2002) (on file with the Washington and Lee Law Review). For a discussion of the FCC policy and possible alternatives, see S. Robert Carter III, *The Sound of Silence: Why and How the FCC Should Permit Private Property Owners to Jam Cell Phones*, 28 RUTGERS COMPUTER & TECH. L.J. 343 (2002).

practices could be made available, as a function of what the individual sought, not what the property owner permitted.

This comparison between 802.11x and 3G implementations should not be read as a policy preference for the latter over the former. In fact, 802.11x technologies may be the best way to provide universal broadband access to the Internet.[161] Moreover, an 802.11x implementation can feature "open access" through legal intervention. For example, local regulations might require all proprietors providing general Wi-Fi services to their customers not to exercise censorship. Security and other self-protection measures[162] could be permitted, but nothing more.

Several real-space analogies to such interventions exist. During the preliminary planning of malls, communities typically place numerous conditions on developers, including financial mitigation—the requirement to contribute certain municipal and regulatory fees—and design requirements—the nature of parking, landscaped set-backs, and exterior architectural treatments.[163] Communications analogies also exist. Consider, for instance, the leased access channel[164] and must carry[165] requirements that fall on cable operators. Both sets of federal regulations require cable operators' "private property" to be partially opened to carry traffic on a common carriage-like basis. Access regulations could also be implemented federally, by the Federal Communications Commission (FCC), which regulates use of the electromagnetic spectrum in the "public interest."[166] Indeed, all the bands that are permitted by the FCC to be used without license could have certain "open access" requirements like the requirements specified above.

To the expected objection that market competition will make all this fretting unnecessary, we respond "maybe yes, maybe no." Although

---

161. *See* ROB FLICKENGER, BUILDING WIRELESS COMMUNITY NETWORKS 3–6 (2002) (providing instructions to create a wireless network for community Internet access).

162. Providers might be concerned that somehow they would be exposed to liability by bad acts done by customers using the Internet access they provided. Under current law, however, these providers receive extraordinarily robust protection under 47 U.S.C. § 230 (2000) (excusing any provider or user of interactive computer services from liability as publisher or speaker of information provided by another information content provider). *See* KANG, *supra* note 125, at 297–306 (providing examples of cases where § 230 immunity protects Internet providers from liability).

163. *See* Berger, *supra* note 61, at 673–75 (describing how local communities often place numerous responsibilities on mall proprietors during the predevelopment stage).

164. *See* 47 U.S.C. § 532 (2000) (regulating cable channels for commercial use).

165. *See id.* § 534 (regulating carriage of local commercial television signals); *id.* § 535 (regulating carriage of noncommercial educational television).

166. *See, e.g.*, *id.* § 303 (outlining FCC powers).

ultimately an empirical question, we are mindful of many contexts in which notwithstanding lack of market power in an antitrust sense, consumers are provided no meaningfully different options across competitors.[167] The reason for this situation is complex and context-specific. Our case for legal intervention is not intended to be definitive. Our goal here is merely to flag the design principle in favor of open access against vertical integration that allows property control to be extended to information control at shopping sites. More interesting possibilities await us in the public sphere by decoupling these two layers.[168]

D. Publicity

When thinking about PerC, the concerns about privacy are obvious, but the converse idea of publicity is not. In order to construct a public sphere, both a public exchange and a *recognized* sharing of experiences must exist. Shared experiences are crucial to developing a sense of common fate and shared future, necessary to lubricate difficult conversations about passionate disagreements. By engaging in similar activities in the public sphere—enjoying a live band together, buying hot dogs from the same vendor, having our children take turns climbing the same jungle gym—we create and understand ourselves as creating a sense of community. These experiences constitute a weak but important social glue. Hannah Arendt pointed out that "our feeling for reality depends utterly upon appearance and therefore upon the existence of a public realm into which things can appear out of the darkness of sheltered existence."[169] The possibility of a public, shared common experience depends upon the "harsher light of the public realm."[170]

---

167. *See* Cohen, *supra* note 109, at 1811 (describing unequal bargaining power as well as standard terms across an industry that offer few options).

168. A rich literature on keeping separate the various layers of communications now exists. *See, e.g.*, Timothy Wu, *Application-Centered Internet Analysis*, 85 VA. L. REV. 1163, 1190–91 (1999) (naming the layers of communication present, for example, in communications between two lawyers or on the Internet); *see also* Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925, 930–31 (2001) (discussing the layers of communication within an end-to-end network design); LAWRENCE B. SOLUM & MINN CHUNG, THE LAYERS PRINCIPLE: INTERNET ARCHITECTURE AND THE LAW 32–33 (2003), *at* http://ssrn.com/abstract=416263 (last visited Oct. 12, 2004) (discussing the "violation of the integrity of layers" and "the layers principle") (on file with the Washington and Lee Law Review).

169. ARENDT, *supra* note 64, at 51.

170. *Id.*

As data become increasingly customized to both the individual and the environment, micro-worlds are established such that each person perceives a different version of the physical realm. That larger context is always individually construed,[171] but PerC allows each individual's micro-world to differ substantially, in ways invisible and inaccessible to others. One person's read-out of a passerby might include criminal record while another person receives marital status. One person's augmented information about the civic center gives its history while another's tells where to pay a traffic fine. Do we share the public sphere in such a scenario, when our data overlays (looking out) function simultaneously as opaque veils (looking in) that undermine the sharing of collective experiences and its public recognition? Such privatized augmentations of reality can fragment the substructure of civility. The environment, as such, divides us into multiple, fragmented publics even as we share the same space.

The proper response is not, however, to reject personalization. Rather, the challenge is to develop counteracting strategies that publicize some portion of our private realities without abandoning privacy. We have already discussed how PerC, by publicizing mutual interests, can catalyze social interaction. Consider a few more examples. Consider the possibility of publicly displaying the average "preferences" that have been set in our flirting profiles. This idea is not much different from being able to see what is the most popular Google search term at any given time. For example, we learn something about our shared selves when that search term switches from "sex" to "war."[172]

---

171. Anupam Chander has well reminded us that in assessing the "fragmentation" cost of highly personalized information environments, we should remember that what was commonly shared in the past may have reflected a burdensome if not oppressive hegemony of the mainstream. Chander, *supra* note 127, at 1484–93.

172. That shift occurred in Britain the day the Iraq war began. In the United States, the most popular search changed from Dixie Chicks (who had stirred up controversy by criticizing George W. Bush) to Iraq, according to Yahoo!. *Surfers Seek War, Not Sex*, TORONTO SUN, Mar. 21, 2003, at 7, *available at* LEXIS, The Toronto Sun File.

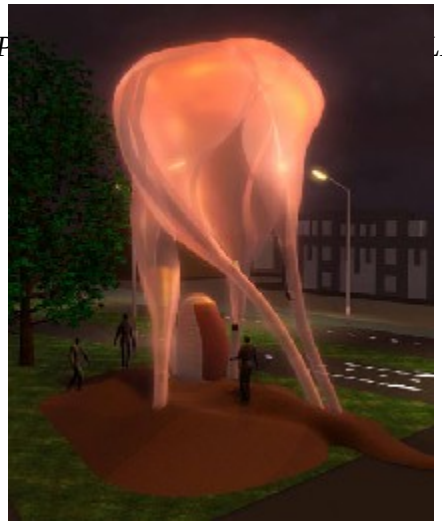

Photo Credit: NOX/Lars Spuyhroek

D-Tower

Consider, as a provocative architectural example, the above animated model structure. In an unrealized project by the designer Lars Spuybroek of the Netherlands, (working with Q.S. Seafijn, 1998–2001) the D-Tower was developed for the city of Doetinchem. The public sculpture's appearance is tied to an online questionnaire about public mood: When the tower is a deep red, we know Doetinchem's citizens are feeling love and happiness more than fear and hate. At the D-Tower's website, browsers can gather more specific information about what fellow citizens are thinking and add their own commentary. While this project is whimsical, it suggests not only a civic role that PerC might play, but also roles for aesthetics and critical art practices, including architecture and sculpture.

Variations on this theme are easy to conjure up. Imagine, for instance, a 9/11 memorial that allows anyone who lost someone in the attacks to tell it so. The memorial could emit a certain song on the basis of such inputs, with volume and duration shaped by number and recency of the input. Like seeing fresh flowers at a tombstone, we could hear something about ourselves collectively as we walk by. We could know that someone recently visited the monument and shared the personal loss with the community in an act of collective intimacy.

In addition to such societal "mood rings," one could imagine using PerC to publicize more concrete information in efficient ways. By aggregating our individual choices and presenting a summary, we could produce collaborative filters that provide valuable self-knowledge to the collective as well as specific recommendations to individual members of that collective. Movie and restaurant recommendations could work just this way. Why not also absentee

voting or its subsequent online variants?[173] Fully peer-to-peer algorithms that produce such publicity while maintaining privacy have already been specified.[174]

Such knowledge might guide not only "smart mob" action, but also influence and speed up the evolution of social norms. Cass Sunstein has pointed out that certain norms, even if not widely held, persist because information about their unpopularity is not publicly exchanged or recognized.[175] If tomorrow's mall can provide different avenues of publicity, while respecting information privacy, then outdated norms might expire faster.

VI. Conclusion

PerC is what happens when the Internet gets physical, when cyberspace "plugs and plays" with the material world. We have a fleeting window of opportunity to engage proactively the ethical, legal, and social issues that will inevitably arise as PerC emerges. Unfortunately, the problems seem intractable, requiring a wide variety of expertise, creativity, and insight for them simply to be grasped much less solved. In addition, society typically responds late, after the technologies have already been embedded into both our material and social infrastructure.

If we are to avoid a constantly reactive posture capable only of post hoc tweaking of details, then the intellectual resources necessary for proactive engagement must be brought to bear on the significant information technology innovations to come. Certain risk is associated with embedding technologies in the public sphere and with embedding the public sphere in our technologies. Since the former is inevitable, our responsibility is to engage the latter as fully as possible.

We have outlined only preliminary thoughts about how to embed responsibly the public sphere with emergent digital technologies. We recommend broad design principles of respecting privacy, increasing transparency, guaranteeing open access, and promoting publicity. Implicit in our entire analysis was a meta-design principle of *embedded responsibility*,

---

173. *See generally* Kang, *supra* note 117, 1167–68 (discussing voting intermediaries).

174. *See, e.g.*, John Canny, Collaborative Filtering with Privacy 3–8, *available at* http://www.cs.berkeley.edu/~jfc/papers/02/IEEESP02.pdf (last visited Nov. 16, 2004) (describing an algorithm that allows users to input preferences confidentially and receive general recommendations) (on file with the Washington and Lee Law Review).

175. *See* CASS R. SUNSTEIN, FREE MARKETS AND SOCIAL JUSTICE 38–40 (1997) (discussing the role of norms and possible cascades).

which suggests that technologies should be developed in such a way that they can limit themselves to comply with relevant, evolving social norms—the promotion of the "public sphere." Wherever possible, the social norms constraining a technology should be able to be implemented through the technology itself or through a corresponding counter-technology.[176] This approach, which requires early integration of ethical, social, and legal norms into the technology, creates a more secure and low-cost architecture than if these features are bolted on after the fact. Indeed, if attempted after a first standard has been constructed, complaints about costs of change will often be justified, since the change will not be integral to the basic design. By contrast, if these issues are considered at the beginning, the cost may not be so large, and features that promote public acceptance of the technology can be embedded.

PerC's potential is vast. The technology will profoundly alter our relationship to our surroundings, our very agency therein. We have laid out the terms as well as some of the objectives that should guide PerC's development as we haphazardly seed the public sphere. With each technological advance, that guidance must grow more explicit.

176. This meta-principle arises from discussions of various workshops at the Institute for Pervasive Computing and Society, at UCLA.