5. UBIQUITOUS COMPUTING AND SPATIAL PRIVACY

ANNE UTECK

I. Introduction 83
II. The technological dimensions and implications 85
  A. Enabling Technologies 85
  B. Ubiquitous Computing (Ubicomp) 88
III. Privacy and space 92
  A. Characterizing the Privacy Interest 92
  B. Anonymity 93
  C. Conceptualizing Space 94
    Territorial Space 94
    Personal Space 95
    Public Urban Space 95
IV. Legal protection 96
V. Conclusion 101

I. INTRODUCTION

In 1991, Mark Weiser envisioned a world in which computing would become an integral part of our everyday experience.[1] This vision assumed a paradigmatic shift, not only in computing, but also in society. Enabling technologies would be everywhere,[2] embedded in everyday things, people, and places. As they are combined, integrated, and connected, invisibly and remotely to networks, we move toward a society characterized by ubiquitous computing (ubicomp).[3]

Emerging location, communication, and mobile technologies, such as Global Positioning Systems (GPS), Radio-Frequency Identification (RFID), and advanced wireless devices enhance and extend the ability to locate and track people and things in the real physical world *anywhere, anytime, accurately, continuously, and in real time*. There are compelling advantages to such capabilities that are important to serving the public interest, as for example, more effective emergency services, security applications by law enforcement, and child safety. The privacy implications, however, are profound. The seamless integration of

1. Mark Weiser, "The Computer for the 21st Century," *Scientific American* 265, no. 3 (1991), http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html.

2. Adam Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing* (Berkeley, CA: New Riders, 2006).

3. Gordon A. Gow, "Privacy and Ubiquitous Network Societies," background paper prepared for International Telecommunication Union, March 2005, http://www.itu.int/osg/spu/ni/ubiquitous/Papers/Privacy%20background%20paper.pdf.

these technologies into the spaces and places of our everyday lives, more directly and more pervasively, compromises physical and social boundaries in private and public spheres. This potential to be caught within a web of constant accessibility, visibility, and exposure challenges our fundamental ideas about personal space and boundaries, and the privacy expectations that accompany them.

The predominant emphasis on the data protection model of information privacy does not address the central spatial threats to privacy implicated by ubicomp technologies. While this next generation of technologies certainly adds a new dimension to data collection, its use also implicates the interests we have in limiting intrusions into our space, movements, and activities so as to be free from observation. While privacy has both spatial and informational dimensions, "linking privacy to informational transparency tends to mask a conceptually distinct privacy harm that is spatial."[4] Without an assessment that more broadly considers people and their spaces, we risk privacy interests with a spatial dimension being collapsed into the informational paradigm, further marginalizing core interests that individuals have in sustaining physical and personal space.

This chapter begins to examine spatial privacy, its nature and scope, and its viability for legal protection. While geospatial technologies create new concerns for consumers, the focus of this chapter is in the context of government conduct and surveillance activity. Section II briefly describes the technologies that are enabling and driving the development of ubicomp, highlights the main features of this new era of computing in everyday life, and identifies the surveillance issues that potentially threaten our noninformational privacy interests in the spaces of our daily lives. These interests and the spaces in which we seek to protect privacy are explored in Section III. Section IV assesses the extent to which law acknowledges and protects spatial privacy under the Section 8 search and seizure provision of the Canadian Charter of Rights and Freedoms.[5] This analysis demonstrates that while Section 8 purports to recognize a reasonable expectation of spatial privacy, it has been narrowly interpreted and fails to take into account the nature of changing technologies and the plurality of realms in which we engage in activities that we seek to protect from ubiquitous surveillance. This chapter concludes by suggesting that we need to develop a construct that better reflects the spatiality central to our experiences of everyday life and our expectations that the spaces in which we live those experiences are protected from unwarranted intrusion.

4. Julie Cohen, "Privacy, Visibility, Transparency and Exposure," *University of Chicago Law Review* 75, no. 1 (2008), http://ssrn.com.abstract=1012068.

5. Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act, 1982* (U.K.), 1982, c. 11.

II. THE TECHNOLOGICAL DIMENSIONS AND IMPLICATIONS

A. Enabling Technologies

Mainstream technology, such as credit and affinity cards, closed-circuit television (CCTV), red-light cameras, biometric systems, tracking software, thermal imaging, and infrared devices, are all forms of surveillance technologies to varying degrees, but have inherent limitations. GPS, RFID, and advanced wireless technologies overcome many of the limitations of the mainstream technologies because they can point to the exact location of a person, and follow movement—in real time—on an ongoing, uninterrupted basis. In effect, these technologies create the potential for directed surveillance throughout the environment of our everyday lives with the ultimate, albeit unstated, goal of monitoring or observing all people in all places all of the time.[6]

GPS[7] has been transformed from a technology used solely for military purposes to a viable real-time, multisatellite network supporting a host of nonmilitary, civilian, and consumer applications. For example, GPS is being used for traffic engineering for the purpose of crash reporting and traffic system performance.[8] Additionally, GPS is being increasingly marketed as a tracking device in vehicles,[9] and for monitoring both employees[10] and parolees.[11]

RFID technology is essentially a microchip, which acts as a transmitter that is embedded in an object or implanted in a person, and is generally used to describe any technology that uses radio signals to identify specific objects.[12] RFIDs, like

6. Martin Dodge, Michael Batty, and Robert Kitchin, "No Longer Lost in the Crowd: Prospects of Continuous Geosurveillance," Association of American Geographers Conference, March 2004 http://www.casa.ucl.ac.uk/martin/aag_geosurveillance.pdf.

7. GPS is a radio navigation system that allows land, sea, and airborne users to determine their exact location, velocity, and time in all weather conditions, anywhere in the world. Mark Monmonier, *Spying With Maps, Surveillance Technologies and The Future of Privacy* (Chicago: The University of Chicago Press, 2002); Waseem Karim "The Privacy Implications of Personal Locators: Why You Should Think Twice Before Voluntarily Availing Yourself to GPS Monitoring," *University of Washington Journal of Law & Policy* 14 (2004) 485; and April Otterberg "GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court's Theory of the Public Space Under the Fourth Amendment," *Boston College Law Review* 46, no. 3 (2005) 661.

8. Monmonier, *Spying With Maps* (n. 7).

9. See for example, Solutions Into Motion Limited Web site, http://www.trackem.com; Fleetboss Global Positioning Solutions Inc. Web site, http://www.fleetboss.com; AirIQ Web site, http://www.airiq.com.

10. J. K. Peterson, *Understanding Surveillance Technologies: Spy Devices, Privacy, History and Applications* 2nd ed., (Boca Raton: Taylor & Francis, 2007), 337.

11. See for example, Pro-Tech Web site, http://www.ptm.com.

12. Simson Garfinkel & Beth Rosenberg, eds., *RFID: Applications, Security, and Privacy* (New Jersey: Pearson Educational, Inc., 2005), 3–36.

GPS systems, are not new, but are being refined and developed for current and potential use in a wide range of contexts.[13] The potential for government use of RFIDs is very broad, in part because of the many roles that governments play in society. Governments may seek to use RFIDs as part of regulatory schemes, in the delivery of service, supply chains, health care systems, or in relation to government employees, such as police officers or military personnel. On Canadian highways RFIDs are used in a prepaid system of highway or bridge tolls,[14] and some RFID systems measure the travel time of motorists.[15] In public transit systems, users pay by waving an RFID-equipped card before a reader at a subway turnstile.[16] With an overriding interest in security and public safety, as issuers of identity and other official documents, governments are contemplating deployment of larger and more powerful RFIDs, including driver's licenses,[17] health cards,[18] passports,[19] and boarding passes.[20] Public libraries are already looking to track their books by embedding chips that will communicate the book's title, the library to which it belongs, and to whom it is signed out.[21]

In the United Kingdom, law enforcement tagged over 600 adults and close to 6,000 juveniles—some as young as twelve—to ensure compliance with bail conditions.[22] Offenders released from prison are also subject to electronic monitoring either as a condition of early release from prison under the Home Detention Curfew Scheme[23] or as a condition of being released on parole.[24] At five Canadian and Mexican borders, RFID-enabled border smart cards are currently being tested to record the entry and exit of visitors who are required to carry the smart card and enroll in the US-VISIT program.[25] And, people are

13. In the consumer context, see Teresa Scassa et al., "Consumer Privacy and RFID Technology," *Ottawa Law Journal* 37, no. 2 (2006): 215.

14. See for example, 407 ETR Web site, http://www.407etr.com; see also Katherine Albrecht & Liz McIntyre, *Spychips* (Nashville: Nelson Current, 2005) 135–143.

15. RFID Journal "RFID Drives Highway Traffic Report," http://www.rfidjournal.com/article/articleprint/1234/–1/1/.

16. Albrecht & MacIntyre, *Spychips* (n. 14).

17. Albrecht & MacIntyre, *Spychips*, 143 (n. 14).

18. Kenneth Fiskin & Jay Lundell, "RFID in Healthcare" in Garfinkel & Rosenberg, *RFID*, 211 (n. 12).

19. United States Department of Homeland Security E-Passports Initiative, http://www.dhs.gov/xnews/releases/pr_1160497737875.shtm.

20. David Fraser, Canadian Privacy Law Blog, http://www.privacylawyer.ca/blog/2006/05/q-what-could-boarding-pass-tell.html.

21. Information and Privacy Commissioner of Ontario, *Guidelines for Using RFID Tags in Ontario Public Libraries*, June 2004, http://www.ipc.on.ca/docs/rfid-lib.pdf.

22. National Probation Service Bulletin, (2006) Electronic Monitoring 6, http://www.probation.homeoffice.gov.uk/output/Page137.asp#Current%20Programmes.

23. In 2005–2006, some 19,000 people were released early under this scheme, *ibid.*

24. *Ibid.*

25. United States Department of Homeland Security Fact Sheet, June 5, 2006, http://www.dhs.gov/xnews/releases/pr_1160495895724.shtm.

opting for RFID implantation. In the United States, some individuals with degenerative brain conditions have also been implanted so that they can be more easily tracked.[26] In another instance, a company chipped two of its employees for workplace access control.[27]

Increasingly important in a world of high mobility, communication is no longer limited while in transit to fixed line. Today, advanced cellular devices do not have to be in use and within range for the location to be identified, but now have tracking capabilities using Automatic Location Identification (ALI) without the necessity that they even be turned on.[28] Wireless Fidelity (Wi-Fi)[29] has also emerged as viable technology for wireless access. This technology is evolving with nodes, or hotspots, as they are known, appearing in locations such as coffee shops, hotels, libraries, educational institutions, and airports. With a Wi-Fi base station, routed to a broadband connection, devices equipped with Wi-Fi wireless network cards can share the Internet connection emanating from the base station. As the number and variety of hotspots grow, wireless Internet service providers hope to create meshed networks of hotspots with the potential to observe and track the physical movement of those connected to the Wi-Fi network. Bluetooth[30] uses similar technology for the purpose of providing interconnection between a wide variety of devices—mobile telephones, PDAs, laptops, even Internet-ready refrigerators or washing machines.[31] Organizations deploy Bluetooth-based locational surveillance systems.[32]

The convergence of the enabling technologies offers complementary strategies to the limitations of each in determining instantaneous location and tracking of people, vehicles, and objects. An RFID system can record location when a subject with an RFID tag passes within range of a compatible reader. An RFID chip with read-write memory and the ability to record location identifiers from transmitters along its path can be debriefed by a system design to reconstruct the subject's route. RFID tracking requires readers positioned at appropriate choke points in

26. See Verichip Corporation, http://www.verichipcorp.com.

27. Richard Waters, "US group implants electronic tags in workers" *Financial Times*, February 12, 2006 http://www.ft.com/cms/s/ec414700-9bf4-11da-8baa-0000779e2340.html.

28. Colin Bennett and Lori Crowe, "Location-Based Services and the Surveillance of Mobility: An Analysis of Privacy Risks in Canada," (2005) *A Report to the Office of the Privacy Commissioner of Canada*, http://web.uvic.ca/polisci/bennett/pdf/lbsfinal.pdf.

29. Colin Bennett and Priscilla Regan, eds, "Mobilities," *Surveillance & Society* 1, no. 4 (2004) http://www.surveillance-and-society.org/journalv1i4.htm; see also Ontario Information and Privacy Commissioner Web site, "Privacy in a Wireless World," 2001, http://www.ipc.on.ca/scripts/index_.asp?action=31&N_ID=1&P_ID=11263&U_ID=0.

30. "Bluetooth and Wireless Technologies," *Intel Technology Journal* 4, no. 2 (2002) http://intel.com/technology/itj/archive/2000.htm.

31. Albrecht & MacIntyre, *Spychips*, 85–95 (n. 14).

32. Pius Uzamere, Simson Garfinkel & Ricardo Garcia, "Bluejacked" in Garfinkel & Rosenberg, *RFID*, 323 (n. 12); See also Bluetooth SIG, Inc. Web site, http://bluetooth.com/bluetooth/.

the circulation network. GPS, on the other hand, allows for continuous tracking, especially if linked in real-time to a wireless mobile system, but because of signal attenuation and multipath corrupted signals in certain areas, GPS does not guarantee reliable uninterrupted tracking.[33] These technical difficulties are diminished with the amalgamation or convergence of RFID, GPS, and mobile technologies because RFID extends GPS tracking capabilities, and mobile devices add the real-time component. This integration of mobile computing devices and communication services means more powerful location-based systems because they can pinpoint coordinates more precisely—continuously and in real time.

Location-based services (LBS) combining location technologies are producing a number of new applications designed to assist government, consumers, employers, parents, and others to "locate" individuals and objects in real time. The telecommunications industry intends to use LBS in order to improve public safety through the E-911 Initiative,[34] to aid law enforcement through the lawful access initiative,[35] and to develop LBS commercial applications.[36] Potential future uses include a networked GPS system right in the home which could pinpoint the whereabouts of people, things, and animals.[37] Currently, many of the individual nodes behind the location systems exist as objects that surround the individual—car, clothing, mobile phones, transit systems, and walls with tag readers. Embedding chips, however, in a wider range of objects—identification documents for example, or even implanted under the skin,[38] especially when coupled with GPS—will further refine and enhance location-based services.

B. Ubiquitous Computing (Ubicomp)

Ubicomp has been defined as "the method of enhancing computer use by making many computers available throughout the physical environment, but

33. While GPS operates on a continuous basis, it is limited to the extent that satellites cannot be transmitted through physical barriers, as for example, underground, in buildings or as a result of topography.

34. Bennett & Regan, "Mobilities" (n. 29).

35. CIPPIC Report, "Lawful Access: Police Surveillance," http://www.cippic.ca/en/projects-cases/lawful-access/.

36. For example, mapping and directory services, fleet management, protection of goods, and shipping management: Bennett and Crowe, "Location-Based Services and the Surveillance of Mobility," (n. 28); see also David Phillips & Michael Curry, "Privacy and the Phenetic Urge: Geodemographics and the changing spatiality of local practice" in David Lyon, ed., *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination* (New York: Routledge, 2003), 137.

37. Bennett and Crowe, "Location-Based Services and the Surveillance of Mobility," (n. 28).

38. Angela Long, "Implanting Dignity: Considering the Use of RFID for Tracking Human Beings" ID Trail Mix, March 27, 2007, http://www.idtrail.org/content/view/656/42/; Thomas C. Greene, "Feds Approve Human RFID Implants," *The Register* (2004) www.theregister.co.uk/2004/10/14/human_rfid_implants/.

making them effectively invisible."[39] Intelligent, intuitive interfaces will make computer devices simple to use and unobtrusive. Communication networks will connect these devices to facilitate and build on the anywhere, anytime paradigm by adding access for all persons and things creating an anytime, anywhere, for anyone, and anything paradigm.

Ubiquitous computing will be everywhere. This is its essence, its explicit goal.[40] Consequently, a ubiquitous system will affect a large—if not every—part of our lives, from crossing a street to sitting in the living room or entering an office building. A key feature of ubicomp is its *invisibility* in the design of everyday living and work spaces.[41] It is, literally, visible (you can physically see and touch a device), yet effectively invisible in everyday spaces and as we go about our activities within those spaces. It is then, difficult for individuals to be aware of the surveillance possibility. The technology not only hides the possibility of surveillance, but it also hides the signs of what is being monitored. Individuals are not always aware of what is being observed, even if they are aware of the installed technology. Apart from hiding the existence of surveillance, the embedded technology also makes it difficult to know what exactly is being observed and monitored. This creates, in effect, an embedded panopticon—pervasive surveillance hidden in the environment. As the technology shrinks and processing power increases, so will the ability of sensors to refine perception of the environment. Thus, observation and tracking will result in a greater degree of accuracy, which translates into greater visibility and exposure of objects and people. This will enable government to interact with devices more naturally and more casually than they do currently, and in ways that suit whatever location or context in which they find themselves, some operating with our expressed permission, others without our permission or our knowledge.[42]

Interestingly, there is no longer the need anymore to surreptitiously install tracking devices on persons, vehicles, or objects because increasingly people carry or use tracking devices voluntarily in their everyday lives. For example, location-determining technology is routinely installed in cell phones and cars. Electronic toll systems, such as the MAC Pass in Nova Scotia,[43] register the presence of each driver who has chosen to install a tag or transponder in her windshield so there is no need for the driver to stop and pay. Such electronically facilitated transactions make driving less burdensome, but at the cost of making

39. Weiser, "The Computer for the 21st Century," (n. 1).

40. Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing*, (n. 2); Marc Langheinrich, "Privacy by Design—Principles of Privacy-Aware Ubiquitous Systems," http://guir.cs.berkeley.edu/pubs/ubicomp2002/privacyworkshop/papers/uc2002-pws.pdf.

41. Langheinrich, *ibid*.

42. It is predicted, in the United States, that by 2014 there will be increasing numbers of arrests based on this kind of government surveillance: Pew Internet and American Life Project, http://www.elon.edu/e-web/predictions/expertsurveys/2004_embeddednetworks.xhtml.

43. Halifax Bridge Commission Web site, http://www.macpass.com.

it less anonymous. This trade-off characterizes numerous other features of evolving "intelligent transportations systems."[44] The same technologies that allow lost drivers to find out where they are, what services are nearby, and how to get where they are also going to potentially allow unseen government observers to watch, learn, and record information.

Radio transmitting devices may also allow officials to observe and trace the paths not only of our phones and cars, but also numerous other tag-embedded products we cannot do without, or choose not to do without. Some people have even voluntarily installed RFID chips into their own bodies or those of their children.[45] And with networked cameras commonplace in many cities, authorities can more easily watch and track people as they walk down a street, even if they are not equipped with a device that emits or receives signals.

The cumulative effect of the emerging technologies and the move toward a world of ubiquitous computing will make it increasingly difficult to evade surveillance. The expansive nature of surveillance made possible by location and tracking technologies "defies the contextualization of life: the workplace, store, and home are no longer separate places in which one is surveilled, but instead each becomes a point on the flow of surveillance."[46] As each of these points becomes increasingly connected to others as a result of technological convergence, more of our everyday lives are exposed. From home, to work, to shop, to take a walk down the street, all these movements and "flows" are subject to scrutiny. The objects we use or carry with us, in turn become tools for surveillance. Movement is no longer a means by which we can evade surveillance, but rather, becomes the subject of surveillance. Such technological transformations bring to physical space many of the same concerns that were raised about tracking movements in virtual space through the use of cookies or Web-click trails. Indeed, "the street itself seems to have evolved into a sensory apparatus."[47]

There is no right not to be observed, but surveillance, regardless of whether or not it is technologically assisted, assaults human dignity and changes behavioral patterns, thereby reducing self-determination.[48] Further, being under the public gaze impairs aspects of individuality that are, or should be, protected in a

44. ITS refers to emerging products, services, and systems, which are based on advanced technologies with enhanced sensory, memory, communication, and information processing capabilities: Transport Canada, http://its-sti.gc.ca/en/what-is-its.htm.

45. Long, "Implanting Dignity," (n. 38); Greene, "Feds Approve Human RFID Implants," (n. 38).

46. Bennett & Regan, "Mobilities," 453 (n. 29).

47. William Gibson, "The Road to Oceania," New York Times, June 25, 2003, http://www.nytimes.com/2003/06/25/opinion/25GIBS.html?ei=5007&en=d57cc2565eb4ec57&ex=1371960000&partner=USERLAND&pagewanted=print&position.

48. Jeffrey Reiman, "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future," *Santa Clara Computer & High Technology Law Journal* 11 (1995) 27, 30.

free and democratic society.[49] And, now well documented, Jeremy Bentham's "Panopticon" as interpreted by Michel Foucault[50] demonstrates the psychological repercussions of being observed and monitored. More recently, the "panoptic geolocator" has been used to describe today's context of surveillance.[51] This may result, for example, in a person being fearful of visiting someone at an AIDS hospice out of concern over being tagged in that location. A chef may worry about bringing a new tag-embedded knife purchased on the way to work on a transit system. Or a student may avoid passing government buildings with research materials on terrorism that have been checked out of the library.

However, even when the observer will not use what is observed in any harmful way or whether anyone is actually watching, there are systemic risks to surveillance. Ubiquitous surveillance alters the experience of space and places producing greater transparency and exposure.[52] In turn, "[e]xposure alters the capacity of places to function as contexts within which identity is developed and performed."[53] As Julie Cohen reminds us, technologies do not exist in a spatial vacuum. These things affect the "lived embodied spaces of real people."[54] We do not give up all expectation of privacy "simply by venturing into a public area"[55] because "privacy results not from locked doors and closed curtains, but also from the way our publicly observable activities are dispersed over space and time."[56] Intrusions into one's life in nontraditional environments "disturbs the victim's daily activities, alters her routines, destroys her solitude, and often makes her feel uncomfortable and uneasy."[57] The question then is what are the privacy interests at risk and what are the spaces in which we expect these interests to be protected?

---

49. Lisa Austin, "The Privacy Interests at Stake in Public Activities" Centre for Innovation, Law & Policy, *Innovate* (Spring 2006): 18, http://www.law.utoronto.ca/documents/publications/Innovate06.pdf.

50. Michel Foucault, *Discipline and Punish: The Birth of the Prison*, A. Sheridon, trans. (New York: Vintage, 1979).

51. Jonathon Weinberg, "RFID, Privacy and Regulation" in Garfinkel & Rosenberg, 83 (n. 12).

52. Julie Cohen, "Privacy, Visibility and Exposure," abstract from conference, *Unblinking, New Perspectives on Visual Privacy in the 21st Century*, Berkeley, November 3–4, 2006, http://www.law.berkeley.edu/institutes/bclt/events/unblinking/unblinking/cohen-unblinking-abstract.htm.

53. *Ibid.*

54. Cohen, "Privacy, Visibility and Exposure," (n. 52).

55. Anita Allen, *Uneasy access: Privacy for women in a free society* (New Jersey: Rowman and Littlefield, 1988), as cited in Gary Marx, "Murky conceptual waters: The public and the private," *Ethics and Information Technology* 3 (1995) 157, 163.

56. Jeffrey Reiman, "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Information Highway Technology of the Future" in B. Rossier, ed., *Privacies: Philosophical Evaluations* (Stanford CA: University of Stanford Press, 2004), 194, 196.

57. Daniel Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review* 154 no. 3 (2006) 477, 549.

III. PRIVACY AND SPACE

A. Characterizing the Privacy Interest

Many formulations of privacy rest on the assumption that there is a "zone" or "realm" into which government may not encroach. A privacy interest in limiting these intrusions is characterized by language of inaccessibility. The concept of limited access recognizes that privacy extends beyond merely being apart from others, to more broadly embracing freedom from scrutiny and intrusions by others.

A number of theorists have advanced limited access conceptions as the underlying basis for protecting privacy.[58] For philosopher Sissela Bok, privacy is "the condition of being protected from unwanted access by others—either physical access, personal information, or attention."[59] According to Ernest Van Den Haag, "[p]rivacy is the exclusive access of a person to a realm of his own. The right of privacy entitles one to exclude others from watching, utilizing, invading, or intruding upon his private realm."[60] And for Ruth Gavison, privacy as limited accessibility concerns "the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention."[61] The extent to which we are known to others refers to the extent of others' knowing information about us. Physical and visual invasions occur when others obtain access to us or when we are the subject of others' attention. Gavison explains what constitutes limited access, which consists of "three independent and irreducible elements: secrecy, anonymity, and solitude."[62] Similarly, under Alan Westin's typology, reserve, anonymity, and solitude are identified as states of privacy.[63] Reserve refers to the creation of a psychological barrier against intrusion. According to Westin, reserve means that you wish to limit accessibility to yourself or communication about yourself to others.[64] Or as Irwin Altman defines, "privacy is selective control of access to the self," including over one's territory and one's personal space.[65] Solitude is being free from observation by others.[66]

---

58. Anita Allen, *Uneasy access* (n. 55); Jeffrey Reiman, "Driving to the Panopticon," (n. 56);. Ruth Gavison, "Privacy and the Limits of Law," *Yale Law Journal* 89 (1980): 421; Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation* (New York: Random House, 1989); Ernest Van Den Haag, "On Privacy" in J. Roland and J.W. Chapman, ed., *Nomos XIII: Privacy* (New York: Atherton Press, 1971).

59. Bok, *Secrets*, 10 (n. 58).

60. Van Den Haag, "On Privacy," 149 (n. 58).

61. Gavison, "Privacy and the Limits of Law," 423 (n. 58).

62. *Ibid.*, 433.

63. Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1970).

64. *Ibid.*, 32–39.

65. Irwin Altman, *The Environment and Social Behaviour: privacy, personal space, territory and crowding* (Monterey, CA: Brooks/Cole, 1975), 18.

66. Solove, "A Taxonomy of Privacy," (n. 57); Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics and the Rise of Technology* (Ithaca: Cornell University Press, 1997).

Recently, Julie Cohen has formulated a variation of accessibility privacy by advancing a theory that characterizes the spatial dimension of privacy as an interest in avoiding or limiting exposure—in other words, a privacy interest against exposure. Under this formulation, "privacy encompasses an interest in the structure of experienced space, and this interest is threatened under conditions of visual or informational exposure."[67]

B. Anonymity

As identified by Gavison and Westin, anonymity is also a key component of privacy. Anonymity is the form of privacy desired when one wishes, or needs, to be among others, but does not want to be personally identified or be the subject of scrutiny or observation.[68] This depiction would typically include an individual's activities in public places or as an individual moves through public spaces, seeking to merge into the "situational landscape."[69] Often even when an individual is in a public place and can be observed by others, the individual does not expect to be "identified and held to the full rules of behavior and role that would operate if he were known to those observing him."[70] The knowledge, or even the apprehension, that one is under observation in public places "destroys the sense of relaxation and freedom that men seek in open spaced and public arenas."[71] An individual is not defending a defined physical, territorial space, but arguably, the intangible personal space within which they wish to limit access to the self.

Anonymity, from another point of view, can also be understood as a positive urban value, even essential to the idea of urbanity. A "society of strangers" is the classical Simmelian[72] interpretation of the urban condition in which urban anonymity equates with freedom. In urban space, people actually expect to remain anonymous.[73] Indeed, as Jacobs points out, "[p]rivacy is precious in cities."[74] Anonymity and privacy in public may actually be a peculiar consequence of modern living in large urban environments. In small communities, one would have little space for being free from surveillance by other community members

67. Cohen, "Privacy, Visibility, Transparency and Exposure," (n. 4).

68. Westin, *Privacy and Freedom*, 32 (n. 63).

69. Melvin Gutterman, "A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance," *Syracuse Law Review* 39 (1998) 647, 706.

70. Westin, *Privacy and Freedom* (n. 63).

71. Westin, *Privacy and Freedom* (n. 63); Richard Posner, "The Right to Privacy," *Georgia Law Review* 12 (1978) 393.

72. Georg Simmel, "The Metropolis and Mental Life" in D. Levine, ed., *On Individuality and Social Forms* (Chicago: University of Chicago Press, 1971), 71.

73. Nick Taylor, "State Surveillance and The Right to Privacy," Surveillance and Society 1, no. 1 (2002): 66, 74, http://www.surveillance-and-society.org/articles1/statesurv.pdf.

74. Jane Jacobs, *The Death and Life of Great American Cities* (New York: Random House Inc., 1961); Reprinted: (New York: Vintage Books, 1992), 58.

or government agents wandering around the town. In urban spaces, however, pervasive public surveillance has serious consequences for the "anonymity in public [that] promotes freedom of action and an open society."[75] Exercising anonymity in a library, a classroom, in a park, or even in a crowded space such as a bus depot, airport, or a bench on a busy street was created by surrounding walls, distances from prying eyes, or by social conventions. However, embedded networked technologies potentially obliterate the spaces and places in which to be anonymous, and also diminish the ability to carry out private activities in public.

C. Conceptualizing Space

Space is a concept that is central to many different areas of study and has varied meanings across a multitude of disciplines. The great variety of possible "types" of space make any definition of space difficult. My aim here is not to construct a theory of space, but, rather, to provide the relevant dimensions of space that are under surveillance and those that implicate privacy interests. Thus, for the purposes of examining spatial privacy in the current technological and legal context, three key categorizations are described here: territorial space, personal space, and urban public space.

Territorial Space The term "territory" generally refers to a particular or indeterminate geographical area. Territorial space is the physical manifestation of something, namely, a physical location.[76] A primary territorial space is one owned by an individual, controlled on a relatively permanent basis and central to daily life. Territoriality is the means of exercising control over this defined physical space.[77]

Territoriality, in its most basic forms, has been defined as a pattern of behavior and attitudes held by an individual that is based on perceived, attempted, or actual control of a definable physical space that may involve habitual occupation, defense, personalization and marking of it.[78] *Marking* means placing an object or substance in a space to indicate one's territorial intentions, and *personalization* means marking in a manner that indicates one's identity.[79] Although a territory is not synonymous with property, territoriality works to control defined spaces and physical places. Thus, territorial space finds architectural and geographical expression whereby control over access serves as a defensible shield to protect privacy.

---

75. Christopher Slobogin, "Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity," *Mississippi Law Journal* 72 (2002) 213, 240.

76. Bryan Lawson, *The Language of Space* (Oxford: Architectural Press, 1999).

77. Julian Edney, "Human Territoriality," *Psychological Bulletin* 81 (1974) 959.

78. *Ibid.*

79. *Ibid.*

Personal Space Spatial dimensions of our lives involve not only constructions of territory anchored in physical space, but also establishing personal zones of privacy.[80] People often expect space from others, even when they are with other people or when in public. We need "personal space" for our psychological well-being.[81] Personal space has been defined as "an area with invisible boundaries surrounding a person's body into which intruders may not come."[82] Personal space differs from other territories in that it is portable, but emphasizes distance for the purposes of exclusion of others.[83] Spatial boundaries are upheld by rules of civility and social respect.[84] We each have certain "territories of the self," and norms of civility require that we respect others' territories.[85]

The Supreme Court of Canada has spoken about a personal zone of privacy, articulating personal privacy as spatial: a person is deemed to be surrounded by a space, but, unlike physical property, this space is not necessarily bounded by tangible barriers.[86] Its realm transcends "the physical and is aimed at protecting the dignity of the human person."[87] Personal privacy can be said to relate to a sphere of the self—a zone of privateness surrounding the individual, which should not be invaded without justification by either unwarranted physical contact or by unwarranted observation.

Public Urban Space Public spaces of cities are the collusion of physical space with the everyday world and have temporary quality in which an individual has occupancy rights.[88] They are multipurpose, accessible spaces which are distinguishable from, and mediate between, demarcated exclusive territories of homes and individuals. These spaces have been described as the surface not in private ownership and are ubiquitous, neutral, and a contingent carrier of urban functions.[89] These areas, sometimes referred to as "in-between" spaces,[90]

80. Simmel, "The Metropolis and Mental Life," 71 (n. 72); Robert Sommer, *Personal Space: The Behvourial Basis of Design* (Englewood, NJ: Prentice-Hall, 1969); E.T. Hall, *The Hidden Dimension* (Garden City, NY: Doubleday, 1966).

81. Altman, *The Environment and Social Behaviour*, 52 (n. 65).

82. Sommer, *Personal Space* (n. 80).

83. *Ibid.*

84. Robert Post, "The Social Foundations of Privacy Community and Self in the Common Law Tort," *California Law Review* 77 (1989) 957, 966.

85. Erving Goffman, *The Presentation of Self in Everyday Life* (New York: Doubleday, 1959).

86. *R v Dyment* [1988] 2 S.C.R. 417 citing *Report of the Task Force established by the Department of Communciations and Department of Justice: Privacy and Computers*(Ottawa: Communication Group, 1972), 428.

87. *Ibid.*

88. Altman, *The Environment and Social Behaviour*, 118 (n. 65); see also, Hille Koskela, "The Cam Era: The Contemporary Urban Panopticon," *Surveillance and Society* 1, no. 3 (2003): 292.

89. Lyn Lofland, *The Public Realm: Exploring the City's Quintessential Social Territory* (IL: Waveland Press, 1998).

90 Eric Paulos, Ken Anderson, and Anthony Townsend, "Ubicomp in the Urban Frontier" conference abstract, September 7, 2004, http://www.paulos.net/intel/pubs/

include, for example, streets, parks, transit routes, libraries, and airports. They are the spaces of everyday lived experience where people work, travel, relax, and interact, hence, both physical and social.[91] Public urban space, then, is a socio-spatial landscape open to, accessible by, and shared among society's members in their multiple roles as individuals, community members, consumers, employees, parents, friends, and citizens. Not only do we spend a significant amount of time in such urban landscapes, but these spaces contribute to our formulation of identity, community, and self.[92]

Public urban space takes on greater significance as new technologies are moving out of structured and enclosed physical environments into urban spaces. The technological embeddedness shifts "the emphasis from abstract information processing to concrete physical space, from clothing and cars to the entire urban landscape."[93] As such, everyday actions and behaviors no longer belong to particular places, and because there is no place—no arena of life which is truly public,[94] private activities can occur in these urban spaces that we may not want or expect to be observed.

IV. LEGAL PROTECTION

The highest legal authority for providing protection of privacy in Canada is the Charter of Rights & Freedoms.[95] While not explicitly granting a right of privacy, the Charter has been interpreted to protect dignity, autonomy, and privacy under sections 7 and 8. Section 7 provides that "Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice." The Supreme Court of Canada has held that the Charter protects a reasonable expectation of privacy as an element of the right to liberty and security of the person.[96] These rights have been taken to guarantee a degree of personal autonomy over decisions affecting an individual's life and protection of the psychological or mental integrity of the individual.[97]

---

papers/Urban%20Frontier%20Workshop%20(UbiComp%202004).pdf.

91. Spiro Kostof, *The City Assembled: The Elements of Urban Form through History* (London: Thames & Hudson, 1992); Rob Krier, *Urban Space* (London: Academy Editions, 1979).

92. Paulos, Anderson, and Townsend, "Ubicomp in the Urban Frontier," (n. 90).

93. Jerry Kang and Dana Cuff "Pervasive Computing: Embedding the Public Sphere," *Washington & Lee Law Review* 62 (2005) 62.

94. Helen Nissenbaum, "Protecting Privacy in an Information Age: The Problem with Privacy in Public," *Law and Philosophy* 17 (1998):559.

95. Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act, 1982* (U.K.), 1982, c. 11 [hereinafter the *Charter*].

96. *R v O'Connor* [1995] 4 S.C.R. 411.

97. *R v Morgentaler* [1988] 1 S.C.R. 30.

While a privacy right has not been fully developed under Section 7, given the potential for increasingly sophisticated surveillance technologies to be used all around us, wider application of its scope and content may take on greater importance.[98] Similarly, the Section 15 equality guarantee provision under the Charter may prove useful to protecting privacy in public. Daphne Gilbert considers privacy in the context of Section 15 in which she proposes the equality provision as "another home" but not "new" home for constitutional protection of privacy interests.[99]

The principal basis for legal recognition of the protection of privacy interests in the context of government activity is Section 8 of the Charter, which provides that "Everyone has the right to be secure against unreasonable search and seizure." The fundamental objective of Section 8 is "to protect individuals from unjustified State intrusion upon privacy"[100] by ensuring them a "reasonable expectation of privacy."[101] It is only where "state examinations constitute an intrusion upon some reasonable privacy interest of individuals does the government action in question constitute a 'search' within the meaning of s.8."[102] Section 8 then guarantees a right to be secure from unreasonable search where the person has a reasonable expectation of privacy. If a person cannot establish that she had a reasonable expectation of privacy, Section 8 will not be engaged. To qualify, a privacy expectation must meet both subjective and objective criteria, the individual must have an actual expectation of privacy, and that expectation must be one that society recognizes as reasonable.[103] Section 8 purports to protect a reasonable expectation of territorial or spatial privacy as one of the zones articulated by the Supreme Court of Canada.[104] This zone of privacy protects physical privacy, but has been de-physicalized so that its protection, at least in theory, extends beyond a property analysis.[105]

Section 8 protection has been characterized as a "broad and general right" to privacy.[106] And in *R v Plant*, the Court confirmed that it is not necessary for a person to establish a possessory interest to attract Section 8 protections.[107] Determining

98. A thorough analysis in this regard is beyond the scope of this chapter.

99 Ian Kerr, *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society* (New York: Oxford University Press, 2009), Chapter 8.

100. *Hunter v Southam Inc.* [1984] 2 S.C.R. 145.

101. *R v Evans* [1996] 1 S.C.R. 8.

102. *R v Tessling* [2004] 3 S.C.R. 432.

103. *Hunter,* 159 (n. 100).

104. The other two zones identified are personal privacy (invasions into the body *R v M (M.R.)* [1998] 3 S.C.R. 393; and informational privacy (protects against the collection of intimate, core biographical information, *R v Plant* [1993] 3 S.C.R. 281; *R v Tessling* (n. 102).

105. *Katz v United States,* 389 U.S. 347 adopted by *Hunter,* 107 (n. 100).

106. *Hunter* (n. 100).

107. *Ibid.*

whether individuals have a reasonable expectation of privacy in a given context is a nuanced, contextual and fundamentally normative exercise. This assessment must be made in light of all the circumstances.[108] All of which envisions that an individual's reasonable expectation of privacy is protected not only within certain well-marked zones or enclaves, but everywhere that circumstances might give rise to such an expectation. This interpretation is supported by *Hunter* in which the Supreme Court of Canada sought to remedy the trespass theory of privacy by linking Section 8 to the protection of "people not places."[109] Such language accords with powerful intuitions about privacy. Many people would probably object to the idea that they relinquish an expectation of privacy simply because they are in a public area. As Jeffrey Reiman points out,"privacy results not from locked doors and closed curtains, but also from the way our publicly observable activities are dispersed over space and time."[110]

If Section 8 then does not protect the privacy of places, but the privacy of the people in those places, it suggests that its protections can move with people as they leave their homes and move from place to place. Section 8 then could be said to protect privacy anywhere that people reasonably expect to have such privacy. Since some people may reasonably expect to be free from ongoing government surveillance even on sidewalks, parks, streets, or coffee shops, Section 8 should have force in these public urban environments as well as in the home or office. This kind of justification has been offered by former Justice LaForest of the Supreme Court of Canada who advised that courts should dispense with "rigid, formalistic borders between private and public spatial domains" and instead attend to what constitutes a "reasonable expectation of privacy in a given context."[111]

Helen Nissenbaum's "contextual integrity" model follows similar reasoning.[112] Rejecting the broadly defined public/private distinction, Nissenbaum's benchmark theory of contextual integrity recognizes that all of the activities people engage in take place in a "plurality of distinct realms."[113] Within each of these realms, or contexts, norms exist, either implicitly or explicitly, which both shape and limit roles, expectations, actions, and practices.[114] Indeed, an emphasis on norms is already at the heart of the reasonable expectation of privacy test because one cannot tell what expectations society is prepared to recognize as reasonable unless one looks at society's practices and specifically privacy norms.[115]

---

108. *R v M (M.R.)*, para 31 (n. 104); *R v Edwards* [1996] 1 S.C.R. 128, para. 30; *R v Wong* [1990] 3 S.C.R. 36, 62; *R v Colarusso* [1994] 1 SCR 20, 54.

109. *Hunter* (n. 100).

110. Reiman, "Driving to the Panopticon," 196 (n. 56).

111. Legal Opinion to then Privacy Commissioner of Canada, G. Radwanski, April 5, 2002.

112. "Privacy as Contextual Integrity," *Washington Law Review* 79, no. 1 (2004) 119.

113. *Ibid.*, 137

114. *Ibid.*

115. Lisa Austin, "Privacy and the Question of Technology," *Law and Philosophy* 22 no. 2 (2003): 119.

The Supreme Court of Canada, however, has yet to strongly reaffirm that Section 8 protects people not places. The *Hunter* framework has only extended to spaces that are in some sense enclosed or marked off by clear boundaries from the outside world. The spatial privacy analysis has largely remained tied to its territorial roots by focusing on the location or place under government surveillance. The persistent tendency toward the territoriality construct is certainly understandable. After all, both property and privacy are inextricably linked to concepts of spatiality and exclusion.

The home—a primary territorial space—remains the dominant place that has attracted a significant privacy interest under Section 8,[116] including nonphysical intrusions through observations by law enforcement agents.[117] However, in *Tessling*, the Supreme Court of Canada found that the privacy of the home extended no further than its external walls.[118] While Binnie J. acknowledged that the territorial privacy interest was implicated, the privacy interest was characterized as "essentially informational" that led to a significantly different result than that of the lower court decision.[119]

The Supreme Court has ventured out to include other locations under Section 8 protection finding that a person is likely to have a reasonable expectation of privacy in hotel rooms,[120] toilet stalls in public washrooms,[121] an apartment,[122] or the perimeter search of a home.[123] However, on the current assessment of spatial

116. *R v Silveira* [1995] 2 SCR 297, per Cory J. "[t]here is no place on earth where persons can have a greater expectation of privacy than within their 'dwelling-house'."

117. *R v Sandhu* (1993) 28 B.C.A.C. 203, 82 C.C.C. (3d) 236, which held that eavesdropping on conversations from outside the home on conversations taking place in a home was an unreasonable search.

118. In *Tessling*, the RCMP arrested a man for running a marijuana growing operation out of his house, which they discovered by using thermal imaging technology to measure the heat emanating from the house. The police did not obtain a warrant for their surveillance activities and the accused brought a s.8 challenge.

119. *R v Tessling*, (2003) 63 O.R. (3d) 1 (CA). The Ontario Court of Appeal followed *R v Kyllo* 533 U.S. 27 (2001), which directly addressed the question of the use of thermal imaging technology by police to photograph patterns of heat escaping from the surface of the home, finding that the warrantless use of FLIR technology violated the Fourth Amendment protection against search and seizure because it was a device not in general public use and it allowed exploration into the home.

120. *R v Wong* (n. 102). But note Lamer's dissent that the hotel room ceased to be a private space when the defendant invited others, including strangers, into the room thus eliminating any reasonable expectation of privacy in that space.

121. *R v O'Flaherty* (1987), 63 Nfld. & P.E. IR 21 (Nfld. CA); *R. v Silva* (1995), 26 O.R. (3d) 554 (Gen. Div.), but note in *R v LeBeau* (1988), 25 O.A.C. 1 (CA) that there is no reasonable expectation of privacy outside the closed toilet cubicles of a public washroom.

122. *R v Pugliese* (1992), 52 O.A.C. 280, but not in common hallways of an apartment building, *R v Laurin* (1997), 98 O.A.C. 50.

123. *R v Kokesch* [1990] 3 S.C.R. 3; *R v Wiley* [1993] 3 S.C.R. 263.

privacy interests, you can still point to barriers that are sustaining its protection, even if law enforcement did not actually trespass. It is, consistently, a tangible barrier that clearly delineates a boundary crossing triggering Section 8. Even in *Tessling*, the Court made clear that this was "off the wall" technology and not "through the wall" technology further reinforcing the tangible barrier basis for sustaining privacy protection. Technologies that enable law enforcement to locate and observe an individual anywhere, at any time operate across all spaces and places without necessarily crossing any tangible boundary, thus, presumably outside the scope of Section 8 protection.

Moreover, within the territorial model of spatial privacy, there is a sliding scale of the level of expectation and degree of privacy the law protects. Hence, a person is entitled to an extremely high expectation of privacy in relation to her residence,[124] and to a much lower expectation in relation to a vehicle in which she is merely a passenger,[125] or an apartment to which one is a visitor.[126] Where the expectation of privacy will fall on the spectrum of places is unclear and difficult to reconcile from a theoretical and practical perspective. If a person has a higher expectation in one physical location and lower in another, then potentially a person who enters, leaves or re-enters physical places or spaces will move up and down the scale during any given period, but potentially being surveilled continuously through those spaces. Observation, tracking, or monitoring made possible by new technologies does not necessarily stop or change because of where you are, but the level of protection may.

The requirement that society recognizes an expectation as reasonable appears to focus less on a person's actions or activities and more on the place in which she acts. In other words, under the current reasonable expectation of privacy test, particular attention is given to the nature of the place in which a person is being observed because this will bear directly upon whether there was a justified expectation of privacy. This is problematic in the context of new technologies that are not always or necessarily deployed or tied to particular places. Clearly, in ubicomp environments technologies are embedded everywhere, thus fluid, mobile, rather than fixed and defined.

Therefore, while the reasonable expectation of privacy standard contemplates the possibility that privacy protection under Section 8 might be made portable and taken with people, it has not been so broadly interpreted. Arguably, the effect has been to further entrench a property analysis, rendering the *Hunter* aspiration unfulfilled. This difficulty is compounded by the ambiguity of the phrase itself, "people, not places." What this phrase actually means remains a mystery and it would, perhaps, have made more sense if this phrase had read "people *and* places." It remains unclear how Section 8 protects people, or rather,

124. *R v Feeney* [1997] 2 S.C.R. 13.
125. *R v Belnavis* [1997] 3 S.C.R. 341.
126. *Edwards* (n. 108).

how it protects people's spatial privacy interests. Does it protect only their physical persons, their words, or activities in enclosed spaces or traditionally private places or does it protect more? Privacy protection encompassed under Section 8 protects "people, not places" but courts have not defined the "space" or the dimensions of privacy that people occupy beyond that which is bounded by traditional perceptions of time and space. Moreover, "people not places" is a problematic foundation because people do rely heavily on the place of an activity in determining whether it is private or not. Deprived of the boundary lines provided by place, courts often resort to factors that weaken privacy protection rather than bolstering it. Courts examine, for example, whether the activity is sufficiently "intimate" to warrant Section 8 protection,[127] a decision that in turn requires controversial judgments about what activities people should and should not have a right to shield from others.

V. CONCLUSION

The powerful new wave of technologies is now being adopted for mainstream use in a variety of contexts. As the full geo-location and tracking capabilities materialize, we are at risk of being more visible and more exposed as we move through the spaces of our everyday lives. The surveillance and privacy implications are profound. However, the current constitutional regime for protecting privacy is less effective in an environment of ubiquitous computing where traditional dichotomies for space, person, and time are easily deconstructed. The parameters of Section 8, namely the territorial spectrum, have been narrowly interpreted by the Supreme Court of Canada. This approach is problematic. As more of our lives and activities are subject to observation by government, the current spatial privacy construct does not take into account all of the spaces in which we carry out private activities nor the nature and effect of the changing technologies rendering irrelevant protections afforded by traditional analysis. The problem is particularly acute where there are no clearly defined tangible barriers to secure protection. The challenge of preserving the privacy interests we have come to enjoy and expect without the fear of being watched and exposed is compounded as the ubiquitous computing agenda moves forward. Central to a ubiquitous networked society is the anytime, anywhere paradigm further contributing to the perception, real or imagined, that we are living in a surveillance society within which the spaces and places for privacy are increasingly vulnerable.

A privacy analysis for the ubiquitous computing age must focus on something other than physical location. This next generation of technology holds vast implications for all of the spaces in which we expect some level of privacy. Indeed,

127. *Tessling* (n. 102); *Plant* (n. 104).

these new forms of ubiquitous systems challenge some of our fundamental ideas about subjectivity, visibility, space, and the distinction between public and private. Together, these challenges necessitate formulating a more nuanced spatial privacy construct that more adequately protects the entire array of privacy interests.