Reconceptualizing Spatial Privacy for the Internet of Everything

E. Anne Uteck

Thesis submitted to the
Faculty of Graduate and Postdoctoral Studies
in partial fulfillment of the requirements
for a doctoral degree in Law

Faculty of Law

Common Law Section

University of Ottawa

DEDICATION

For Carole Lucock

We began together, we shared it together, we finish together.

This is our accomplishment my friend.

ACKNOWLEDGEMENTS

With the biggest and deepest love rushes and profound thanks to my children Spencer and Kate who bravely left their lives in Halifax to come with me to Ottawa on this crazy quest of mine to get a PhD.

Being at the University of Ottawa Faculty of Law, and most especially the opportunity to be involved with the inter-disciplinary research project, 'On the Identity Trail: Understanding the Importance and Impact of Anonymity and Authentication in a Networked Society' has been an invaluable experience. Part of this experience was the opportunity to meet and work with two wonderful individuals and talented scholars, Jane Bailey and Val Steeves. They have enriched my life in Ottawa and provided an exemplary research standard to which we should all strive to attain. And they are, quite simply, just plain fun to be around.

My heartfelt thanks to Teresa Scassa for her constant support and encouragement over the years in Halifax and in Ottawa – and regularly bringing perspective back into the life of a doctoral candidate. I could not have made it this far or accomplished what I have without Teresa Scassa. I have benefitted from her mentorship and value our friendship.

I would also like to thank the external examiner, Dr. Gregory Hagen and all the committee members for participating in this process. I appreciate each of their thorough, insightful and thoughtful commentary.

I also wish to acknowledge and express my thanks for the opportunities, support and assistance that I received in connection with this dissertation from Gowling LaFleur & Henderson LLP, the Social Sciences and Humanities Research Council, and the University of Ottawa. A special thank you to Florence Downing in the Graduate Studies Office at the University of Ottawa Law School who was always calm, efficient, kind, knowledgeable and abundantly helpful.

And, especially, my very deepest and most sincere professional and personal thanks to my supervisor, Ian Kerr, for the guidance, assistance and encouragement he provided in spades throughout the project. I was so fortunate to have had the opportunity to work with Ian Kerr, a gifted, creative and inspiring individual and scholar.
During the personal challenges in this journey, Ian Kerr gave me the strength, resolve and constant support to finish this project.
Above all, working with Ian Kerr was a privilege and our friendship a joy.

ABSTRACT

Twenty years ago, a team of Silicon Valley researchers, led by computing scientist Mark Weiser, envisioned a world in which computing would become an integral part of our everyday experience. Today, this vision is being realized. As technologies are combined, integrated and connected to networks, we are moving to a society characterized by "ubiquitous computing" — a paradigm used to describe pervasive technological embeddedness; from things, to people, to places. Enabling technologies, such as Global Positioning Systems (GPS), Radio-Frequency Identification (RFID) and advanced wireless devices are being introduced and woven into the fabric of our daily lives. With these convergences emerges the unique ability to locate and track people and things anywhere, anytime—including real-time. There are compelling advantages to such an enhanced surveillance capability serving important public interests. Yet, bringing computing technologies beyond the desktop and into the everyday physical world more directly and more pervasively compromise the spaces and places of our lives, challenging our fundamental ideas about spatial boundaries and the privacy expectations that accompany them.

This dissertation examines these issues with the aim of reconceptualizing spatial privacy so that it is capable of sustained, effective legal protection in a world of ubiquitous computing.

Chapter One provides a detailed study of the technological landscape, highlighting three key characteristics of ubiquitous computing: (i) physicality, (ii) invisibility and (iii) context-awareness. Having examined what is considered the "next wave" of computing technology. Chapter Two explores the quantitative and qualitative changes in surveillance activity facilitated by ubiquitous computing. It identifies and discusses the emerging privacy implications raised by ubiquitous surveillance technologies, asserting the increasing importance of reconceiving spatial privacy as computing technology becomes physically embedded in the real world. Chapter Three examines the conceptual and legal privacy landscape, surveying leading privacy theories in order to articulate the array of underlying values and interests. This survey

includes not only privacy scholarship but also privacy jurisprudence, principally as it has been developed under section 8 of the *Canadian Charter of Rights and Freedoms*. Central to this dissertation, this analysis demonstrates the extent to which current privacy law is not adequate to protect the spatial dimension of privacy. Addressing this deficit, Chapter Three calls for a reconceptualization of the traditional category of territorial privacy so that it is capable of sustaining effective legal protection. This conceptual reformation of spatial privacy begins in Chapter Four, which provides a multi-disciplinary investigation of the meaning of place. It adopts an experiential conception developed within the field of Humanistic Geography, better reflecting the spatiality and interactive nature of our everyday lives. Based on this foundation, a new conceptual construct of 'peopled places' is proposed in order to overcome the extent to which the law is currently constrained by its reliance on traditional geography and property concepts. Chapter Five develops the peopled places construct around four defining features: (i) embodiment; (ii) contextual dimensions; (iii) mobile interactions; and (iv) boundary management. Having built an alternative conceptual apparatus, Chapter Five provides legal examples that illustrate how the peopled places construct will better accommodate privacy interests in an environment of pervasive computing. By promulgating an approach that demands spaces to be understood not as empty vessels but as peopled places, this dissertation affirms, clarifies and elaborates the Supreme Court of Canada's long standing intention to remedy the trespass theory of privacy by linking section 8 of the *Charter* to the protection of "people not places".

TABLE OF CONTENTS

INTRODUCTION

It's the next phase, new wave, dance craze, anyways
It's still rock and roll to me

Billy Joel (1980)

Some 20 years ago, inspired by the social sciences,[1] and influenced by computing pioneers before him,[2] PARC chief technologist Mark Weiser articulated a vision of the future in which computing resides in the human world as a natural and integral part of people's interactions and experience in their everyday lives.[3] Unlike the conventional technology-centric model of computing, the future of computing, as Weiser envisioned, was human-centered; reflecting the way humans interact with the physical world.[4] Thus the shift began from a traditional technical view of computational things towards a socio-cultural perspective of the relationship between

---

1 In particular,anthropologist Lucy Suchman, *Plans and Situated Actions: The Problem of Human-machine Communication* (Cambridge, UK: Cambridge University Press, 1987); philosophers, for example, Michael Polanyi, *The Tacit Dimension* (London: Routledge, 1966); Martin Heidegger, *Being & Time*, John Macquarrie, trans. (NY: Harper & Row, 1962) Ludwig Wittgenstein, *Philosophical Investigations* 2nd ed., Anscomble, trans. (Oxford: Blackwell, 1999)*;* and psychologist JJ Gibson, "The Theory of Affordances" in Robert Shaw & John Bransford, eds, *Perceiving, Acting & Knowing: Toward Ecological Psychology* (Hillsdale NJ: Lawrence Erlbaum, 1977) 67.

2 For example, Charles Babbage dreamt of a computing machine whose purpose was to provide both trouble-free and trustworthy applications, serving the human beings and facilitating them in their daily life routines: *On the Economy of Machinery and Manufactures,* 4th ed (London: Frank Cass & Co., 1963); Vannevar Bush perceived the idea of everyday computing, albeit limited given technology at the time, describing his information machine as 'memex' upon which the desk metaphor originated: "As We May Think" *The Atlantic* (July 1945) <http://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/3881/>; Alan Turing to a lesser extent, but what he envisaged was computers involved in activities that could replace humans in performing specific if not all tasks: "Computing Machinery and Intelligence" (1950) 236 Mind 433-460; J.C.R. Licklider began the investigation of human-computer interaction: "Man-Computer Symbiosis" (1960) Trans. on Human Factors in Electronics 1; Nicholas Negroponte at MIT Media Lab was also working on the third wave of computing, but he and Weiser disagreed on its defining features in late 1990's. For Negroponte it was about 'intelligent agents' and for Weiser, this computerized "butler" who was smart and answered our every need was distracting and intrusive. Instead, Weiser advocated interaction and augmentation: "Open House" in Interactive Telecommunications Program (ITP) Review NYU March 1996, online: <http://www.itp.tsoa.nyu.edu/~review/>; see also Nicholas Negroponte, *Being Digital* (New York: Random House, 1995).

3 Mark Weiser, "The Computer for the 21st Century" (1991) 265:3 Scientific American 94.

4 Gregory Abowd & Elizabeth Mynatt, "Charting Past, Present, and Future Research in Ubiquitous Computing" (2000) 7:1 ACM Transactions on Computer-Human Interaction 29 at 32.

humans and computers.[5] Weiser called the new paradigm 'ubiquitous computing,' or ubicomp.[6]

Ubiquitous computing is the field of Human-Computer Interaction (HCI) that seeks to augment everyday objects and physical environments with invisible and networked computing functionality, thus providing the technical and conceptual means for enabling anytime, anywhere computing.[7] Unlike the desktop paradigm, in which a single user consciously engages a single device for a specialized purpose, someone 'using' ubiquitous computing engages many computational devices and systems simultaneously in the course of everyday activities, and may not necessarily be aware they are doing so. Instead of one great disembodied world to be entered through the looking glass of a desktop computer screen,[8] the ubiquitous computing paradigm brings things back into our real world sites and situations of everyday life.

Whether considered a technological revolution or simply an evolution, the next era of computing is a changing world – changing computers, changing lives and changing society. Today, as emerging technologies find their way into the mainstream population, "the future is here and it's in your pocket."[9] We have entered the third wave of computing,[10] evidenced by the now common-place use of mobile personal devices, wireless communication infrastructures, the increasingly widespread use of Radio-Frequency Identification (RFID) embedded in things and people, and location-

---

5 Mark Weiser "The Technologist's Responsibilities and Social Change" (1995) 2:4 Computer Mediated Communication Magazine 17.

6 Weiser, "The Computer for the 21st Century" *supra* note 3.

7 Andrew Sears & Julie Jacko, eds, *The Human-Computer Interaction Handbook*, 2nd ed (Boca Raton, FL: CRC Press, 2007); Constantine Stephanidis & Julie Jacko, eds, *Human Computer Interaction: Theory & Practice* (Mahwah, NJ: Larence Erlbaum Assoc. Inc., 2003); Alan Dix, Janet Finlay, Gregory Abowd & Russell Walker, *Human-Computer Interaction*, 3rd ed, (Englewood Cliffs, NJ: Prentice-Hall, 2003); Brad Myers, "A Brief History of Human-Computer Interaction Technology" (1998) 5:2 ACM Interactions 44.

8 John Walker, "Through the Looking Glass" in Brenda Laurel, ed, *The Art of Human Computer Interface Design* (Reading, MA: Addison-Wesley, 2001) 439.

9 Erin Biba, "Inside the GPS Revolution," *Wired* 17:02 (February 2009) 64; see also Paul Dourish & Genevieve Bell, "Yesterdays Tomorrows" (2007) 11:3 Personal and Ubiquitous Computing 133-143.

10 There appears to be some discrepancy about who actually coined ubiquitous computing as the third wave of computing as some attribute PARC technologist Alan Kay, but Mark Weiser and John Seely-Brown summarized the modern computer history by three trends and the corresponding relationships between computers and us: first, the mainframe (one to many); second, the personal computer, or PC (one to one); and third, ubiquitous computing, or ubicomp, (many to one): Mark Weiser & John Seely-Brown, "Designing Calm Technology" (1996) 1:1 PowerGrid Journal, online:< http://www.powergrid.electriciti.com1.01>.

aware computing in vehicles and devices enabled by Global Positioning Systems (GPS).[11]

By 2020, it is predicted that the ubiquitous networked society will be realized.[12] By 2050, as "things that think want to link,"[13] ubicomp will be at the core of ambient intelligence[14] or the more popular descriptive paradigms of the 'internet of things'[15] and 'everyware.'[16] Thinking will become a distributed function spread across multiple devices, many of them having little to do with our common notion of a computer. Everything will think – buildings, cars, furniture, clothing, bathtubs, pop cans, toilets and toasters – and increasingly, everything will share thoughts and locations across ever-expanding networks in the spaces and places of our everyday lives. In other words, everyday objects will sense, analyze, act and communicate in ways that engage with the world, with people and with things. These are key functions to the realization and effectiveness of the original vision of ubiquitous computing. These same key functions are what render ubiquitous computing technologies inherently privacy-

---

[11] Radio-Frequency Identification (RFID) is essentially a micro-chip, which acts as a transmitter that is embedded in an object, and is generally used to describe any technology that uses radio signals to identify and locate specific objects. Global Positioning Systems (GPS) is a radio navigation system that allows land, sea and airborne users to determine their exact location, velocity and time. GPS, like RFIDs, are not new, but have been refined and developed for current and future use in a wide range of contexts. For a comprehensive discussion on the history and nature of these technologies, see for example, Simon Garfinkel & Beth Rosenber, eds, *RFID: Applications, Security and Privacy* (New Jersey: Pearson Educational Inc., 2005); and Mark Monmonier, *Spying With Maps, Surveillance Technologies and the Future of Privacy* (Chicago: Chicago University Press, 2002).

[12] Richard Harper et al, "Being Human: Human-Computer Interaction in the Year 2020" (Cambridge: Microsoft Research, 2008), online: http://research.microsoft.com/hci2020/downloads/BeingHuman_A4.pdf.>. See also Marta Kwiatkowska et al, eds, "From Computers to Ubiquitous Computing by 2020" (2008) 366 Phil Trans. of the R. Soc. A 3663-3664

[13] Attributed to Nicholas Negroponte in Kenneth Cukier, "A World of Connections: A Special Report on Telecoms" *The Economist* (28 April 2007) 1.

[14] Ambient Intelligence builds on ubiquitous computing and human-centric computer interaction and is characterized by systems or technologies that are embedded, connected, context-aware, personalized, adaptive and anticipatory. See for example, Lara Srivastava et al, *digital.life: ITU Internet Report 2006* (Geneva, International Communication Union, 2006) online: ITU http://www.itu.int/osg/spu/publications/digitalife/> and Hideyuki Nakashima et al, eds, *Ambient Intelligence & Smart Environments* (New York: Springer, 2009).

[15] Bruce Sterling, *Shaping Things* (Cambridge, MA: MIT Press, 2005).

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

sensitive because computing in everything and everywhere facilitates enhanced surveillance practices in our everyday lived spaces.

Certainly, ubicomp adds a new dimension to data collection and informational privacy, but also implicates more directly and more pervasively the spatial interests privacy seeks to protect, interests that have been largely marginalized in privacy law and scholarship. Moreover, limiting privacy analysis to an informational approach serves to reduce, rather than strengthen, privacy protection.

This dissertation responds to pressing socio-legal concerns raised by an increasingly embedded, invisible and networked society by examining ubiquitous computing, the extent to which current analytical approaches to privacy protection are inadequate and proposing an alternate conceptual approach to spatial privacy capable of being applied in law. The conceptual construct of 'peopled places' is proposed as a means of better understanding the spatiality central to our experiences of everyday life and our privacy expectations in the places where we live those experiences. As a conceptual basis, peopled places can provide the lens through which to understand the notion of place and, in future research, as a tool for discussing a legally effective model of spatial privacy.

To meet these goals, this dissertation asks the following questions:

1. What is ubiquitous computing?
2. In what ways does ubiquitous computing raise a new and different set of implications for surveillance and spatial privacy?
3. To what extent do current conceptual and legal frameworks address spatial privacy?
4. What theoretical perspectives on space and place can inform our understanding of people and their environment to support a new conceptual construct of spatial privacy?
5. What shape will this new construct take and what, by way of example, will it do for constitutional privacy law?

To answer these questions, this dissertation is structured as follows: Chapter One, "The Technology Landscape," begins by revisiting ubiquitous computing as envisioned by Mark Weiser for the purpose of framing this dissertation. Framing the discussion around Weiser's original vision of ubiquitous computing is important

because computing science and technologists are informed by and still rely on his key ideas in computing and technology design and development. The objective of Chapter One is to provide a thorough understanding of ubiquitous computing and demonstrate the shift in computing from the desktop model to everyday computing. It is organized and presented around what was identified and determined to be its three defining features: physicality, invisibility and context-awareness. In doing so, the research compiles various aspects of this new computing paradigm, taking the examination of the technological landscape to another level of study and understanding beyond its technical basis. Chapter One concludes by highlighting the key trends and applications as ubiquitous computing moves from vision to reality. In sum, many claim that technology is changing too fast to keep up. Instead, the premise of this dissertation is that Mark Weiser envisioned a paradigm that has been developed over the last twenty years. It is constantly being refined for different implementations, but in essence, the core technology is in already in place.

From the outset, privacy was identified by Weiser as key among the issues raised by ubicomp when "hundreds of computers in every room, all capable of sensing people near them and linked to high-speed networks, have the potential to make totalitarianism up to now seem like sheerest anarchy."[17] Since then, on-going development and progress in computing technologies and network connectivity have deepened the privacy implications first articulated by Weiser. Within the context of growing technological convergence, ubicomp enhances and extends the ability to locate and track people and things anywhere, anytime, accurately, continuously and in real time. Chapter Two, "Surveillance and the Privacy Implications of Ubiquitous Computing," outlines the key qualitative changes in surveillance activity being facilitated by ubicomp and in this context, discusses the emerging privacy implications. This chapter is not intended to be an in-depth study of surveillance since a deeper sociological analysis within surveillance studies is largely outside the scope of this project. The narrower objective of Chapter Two is to show the extent to which ubicomp

[17] Weiser, "The Computer for the 21st Century" *supra* note 3 at 98.

enhances surveillance capabilities not just with respect to data capture, but also its implications for the spatial dimensions of privacy. The technological embeddedness in bodies, homes and the public sphere demonstrate potentially greater accessibility into places, hence greater exposure of people.

It might be argued that a more robust conception of informational privacy could address the implications raised by ubiquitous computing and enhanced surveillance. However, this dissertation takes the view that an approach that limits analysis to the nature and quality of the information being gathered does not take into account the physical and personal lived spaces which are increasingly left vulnerable by enhanced surveillance enabled by the net generation of computing technologies. And further, an informational approach, on its own, serves to constrain a robust discussion of privacy, whereas a robust discussion of spatial privacy enhances and potentially broadens the legal protection of the array of privacy interests at stake. Ultimately, when other people can take control over one's information they take away control over their private space.

If spatial privacy is being compromised, what is it and to what extent is it being protected in law? Chapter Three, "The Privacy Landscape," considers the conceptual and legal foundations of privacy with particular focus on the spatial dimensions. First, this chapter canvasses the main conceptions of privacy. Although ubiquitous computing represents yet another technology shift influencing our understanding of what privacy is and how it is or ought to be protected, the aim in this chapter is not to construct a new theory of privacy. Rather, this discussion draws attention to the underlying justifications in support of the broad array of privacy interests. All, to a greater or lesser extent, have prompted a rethinking of our attitude toward privacy, but ultimately, the underlying values that privacy seeks to protect reinforce the need for an effective spatial privacy construct. The more critical part of Chapter Three examines privacy jurisprudence under Section 8 of the *Canadian Charter of Rights and*

Freedoms[18] and to a lesser extent, the American search and seizure counterpart, the Fourth Amendment.[19] While spatial privacy issues arise and apply in many contexts, the increasing use of surveillance technologies by law enforcement to search people, places and things raises particularly pressing issues for constitutional privacy law. The focus of this dissertation, therefore, is privacy jurisprudence as principally developed by the Supreme Court of Canada under search and seizure law.

Canadian law, under Section 8 of the *Charter* recognizes a reasonable expectation of territorial privacy as one of the zones articulated by the Supreme Court of Canada.[20] This zone of privacy seeks to protect "an individual's privacy interests in a particular geographic space"[21] but has been de-physicalized so that its protection, at least in theory, extends beyond a property analysis.[22] Section 8 protection has been characterized as a "broad and general right" to privacy.[23] And in *Plant*, the Court confirmed that it is not necessary for a person to establish a possessory interest to attract Section 8 protections.[24] Determining 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;[25] 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

---

[18] Section 8 provides that "everyone has the right to be secure against unreasonable search and seizure." *Canadian Charter of Rights and Freedoms*, Part 1 of the *Constitution Act, 1982*, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11 [*Charter*].

[19] The United States Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." US Const., amend. IV.

[20] The other two zones are personal privacy (invasions into the body *R v M (M.R.)* [1998] 3 SCR. 393 (SCC) [*M (M.R.*)]; and informational privacy (protects against the collection of intimate, core biographical information, *R v Plant* [1993] 3 SC. 281 (SCC) [*Plant*]; *R v Tessling* [2004] 3 SCR 432 (SCC) [*Tessling*].

[21] Teresa Scassa, "Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy" (2010) 7:2 CJLT 193-220, 199.

[22] *Hunter v Southam Inc* [1984] 2 SCR 145 (SCC) [*Hunter*]. In *Hunter*, the Court "ruptured the shackles that confined [section 8] claims to property." *R v Dyment* [1988] 2 SCR 417, 428(SCC) [*Dyment*].

[23] *Hunter, ibid* at 158.

[24] *Plant, supra* note 20.

[25] *R v M (M.R.)*, *supra* note 20 at para 31; *R v Edwards* [1996] 1 SCR 128 at para. 30 (SCC) [*Edwards*]; *R v Wong* [1990] 3 SCR 36 at 62 (SCC) [*Wong*]; *R v Colarusso* [1994] 1 SCR 20 at 54 (SCC) [*Colarusso*].

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."[26] Such language accords with powerful intuitions about privacy since most people would probably object to the idea that they relinquish an expectation of privacy once outside a bounded space. 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."[27]

The *Hunter* aspiration, however, has not been fulfilled and the parameters of privacy protection have been narrowly interpreted. By remaining tied to its territorial roots, the current conceptual and legal construct does not take into account the nature of changing technologies; the effect and implications of physically embedded technologies across the plurality of realms in which we expect to be free from ubiquitous surveillance. Some places may be protected if trespass occurs, but the current framework leaves people largely unprotected in a computing environment where no physical intrusions occur. Part of the challenge and complexity in responding to this current deficiency in law is how to conceptualize and situate notions of place when ubiquitous computing is reshaping, and potentially redefining, the environments in which we move, live, interact, play, travel and work.

The examination in Chapter Three, and later elaborated on in Chapter Five, shows the limitations in current legal approaches to adequately protect privacy interests. In particular, reliance on the current territorial model of spatial privacy continues to constrain effective legal protection. If privacy is to protect people, it must protect them in their lived spaces. Although courts have consistently said privacy protects people not places, people are always in some place. But that place is not limited to being behind closed doors, but everywhere and it is not just people that are everywhere, but now computing is everywhere. What is required, therefore, is an

---

[26] *Katz v United States,* 389 US 347 [*Katz*] adopted by *Hunter, supra* note 22 at 107.

[27] Jeffrey Reiman, "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Information Highway Technology of the Future" in Beate Rossler, ed, *Privacies: Philosophical Evaluations* (Stanford, CA: University of Stanford Press, 2004), 194-214, 196.

alternate conceptual construct of 'place' that better reflects our experiences and expectations in everyday life. Peopled places is proposed in order to overcome the extent to which the law is currently constrained by its reliance on traditional geography and property concepts to define the meaning of place. Developing the conceptual construct of peopled places will contribute to privacy law scholarship by offering a way that invigorates spatial privacy rather than diminish it.

Chapter Four, "What is Place," begins the building process of an alternative construction of place to inform and shape – and be shaped by – privacy law, by investigating the meaning of place. The principal aim of this chapter was to show an evolution in scholarly thinking on place outside traditional geography and establish a basis for conceptualizing place beyond a data location or simply by defined parameters. It sets out to distinguish the concepts of space and place and then lays the theoretical groundwork informing the humanist approach to the meaning of place. This dissertation supports a humanist approach to defining place because it better reflects our everyday lives and the privacy expectations that accompany them. For geography scholar Yi-Fu Tuan, "place incarnates the experiences and aspirations of people. Place is not only a fact to be explained in the broader frame of space, but it is also a reality to be clarified and understood from the perspectives of the people who give it meaning." [28]Ultimately, this type of analysis to the meaning of place accommodates the *Hunter* aspiration of privacy is meant to protect people.

In terms of a theoretical grounding and clarification of what is meant by place, the task is a complex one as the notion of place does not lend itself to simply providing a definition and underlying explanations. It seems something of a truism to say that what is closest and most familiar to us is often that which is most easily overlooked. Once you get beyond space in its most formal and familiar sense, reviewing space and place discourse is a daunting exercise. The seemingly infinite types of space and many dimensions of place that have been examined by a multitude of disciplines appear to be layered upon one another or contained within the next, and interwoven with other

---

[28] Yi-Fu Tuan, *Space and Place: The Perspective of Experience* (Minneapolis: University of Minnesota Press, 1977) 387.

concepts. This chapter highlights the key thematic signposts within classic, scientific and traditional geographical discourse as these theories largely inform current legal approaches to protecting spatial privacy.

Phenomenology provides a theoretical foundation that supplements abstract thinking about space with an understanding of the role of the body and the physical environment. The phenomenological perspectives inform environmental psychology, one of the first academic disciplines to address not just physical space that surrounds us, but with the way physical space, and place, is related to and influenced by human activities. All of these accounts share a human-centered conception of space, moving away from the ideas of space as a mere container, or place as simply a location, considering instead space as a setting for human activity and experiences. Influenced by this alternative spatial thinking, the concept of place is rediscovered in geography.

Chapter Four adopts an experiential conception of place as primarily developed within humanistic geography because it takes a pragmatic view to understanding people's experience in a physical environment within which the notion of 'place' is further developed. Its vision sees 'space' as an abstract geometrical extension and location whereas place describes our experience of being in the world and investing a physical location or setting with meaning. While acknowledging the continued significance of space as structural, the Humanists' commitment to people and their making of place based on the lived nature of spaces in the real world serves as a strong conceptual grounding for building a new spatial construct to sustain privacy protection of these interests.

Building on these ideas, Chapter Five, "Legal Protection of Peopled Places: From Territorial to Spatial Privacy," the conceptual construct of 'peopled places' is developed. This chapter is divided into two parts. Part One begins by identifying the importance of moving beyond the language of territory to the language of people's lived and spatial experiences. In other words, abandoning the label of 'territorial privacy' and more definitively and consistently utilizing 'spatial privacy' so as not to limit privacy discourse. Part One of this chapter then develops the alternative conceptual construct of peopled places around four defining features viewed as

effectively integrating and capturing the emerging computing environment and the plurality of realms in which people live and interact. These defining features are, embodiment because when we experience a place we do so, first, through our body. Second, the broader physical and social contextual dimensions where human activities make sense and contribute to their meaning. The broader physical context refers to extending the meaning of place beyond the jurisprudential focus on the sanctity of the traditionally defined home. With respect to the social context, although seemingly incompatible with the phenomenological perspective on the experience of a sole person, people are also created through social interaction. Thus, the experiential meaning of place is expanded by incorporating sociological insights. In this way, the focus of the peopled places construct is on lived experiences. Third, mobility because people and computing are on the move. And finally, the fourth defining feature of peopled places is boundary management. Although some sense of boundary is important in understanding peopled places, the current and enduring traditional private-public paradigm does not adequately address the issues raised in this dissertation. Acknowledging the permeable nature of these concepts may be more productive than abandoning them altogether. Although a fully articulated theory of boundary management is beyond the scope of this dissertation, emerging scholarship in law[29] and computing science[30] have begun to consider and build upon the earlier boundary work of Alan Westin[31] and Irwin Altman[32] to address both informational and spatial privacy issues.

Having set out the conceptual framework of people places, in Part Two of Chapter Five, peopled places seeks to leverage the law's lost opportunities by

---

[29] See for example, Julie Cohen, *Configuring the Networked Self: Law, Code and the Play of Everyday Practice* (New Haven, CT: Yale University Press, 2012); and Kirsty Hughes, "A Behavioural Understanding of Privacy and its Implications for Privacy Law" (2012) 75:5 Modern Law Review 806-836.

[30] See for example, Leysia Palen & Paul Dourish, "Unpacking Privacy for a Networked World" in *Proceedings of the SIGCHI On Human Factors in Computing Systems* (New York: ACM Press, 2003) 129-136; and Sandra Petronio, *Boundaries of Privacy: Dialetics of Disclosure* (Albany, NY: State University of New York Press, 2002).

[31] *Privacy and Freedom* (New York: Atheneum, 1970).

[32] *The Environment and Social Behaviour: Privacy, Personal Space, Territory and Crowding* (Monterey, CA: Brooks/Cole, 1975).

providing examples of how this new construct will better accommodate privacy interest in an environment of pervasive and ubiquitous computing. Central to the development of peopled places is the 1967 United States Supreme Court decision in *Katz*.[33] But not necessarily for the reasons most people attribute it landmark status; the reasonable expectation of privacy test.[34] Rather, the significance of *Katz* for the purposes of developing a new spatial construct of privacy is in its recognition that if in the past the paradigmatic private place was the home, it has since moved to the telephone booth and beyond. This has largely gone unnoticed by both American and Canadian courts, rendering it difficult for law to move beyond the traditional understandings of geographic space and place. Yet, one of the most pressing issues is technology enhanced surveillance by police. Thus, Chapter Five offers legal examples to illustrate how the peopled places construct might better accommodate privacy interests in an environment of ubiquitous computing.

And finally, in the Conclusion, a brief summary of the key points from each chapter of this dissertation is provided.

Overall, the contributions this project makes are, first, with respect to computing science scholarship, the degree to which it has considered the privacy implications of ubicomp are largely limited to data protection. This work contributes by informing this field of study of a different privacy perspective that needs to be considered in the design and implementation of emerging technologies. Second, this work contends that an informational approach to privacy analysis reduces legal

---

[33] *Katz*, *supra* note 26. In this case, Charles Katz used a public pay phone booth to transmit illegal gambling wagers. The FBI was recording his conversations via an electronic eavesdropping device attached to the exterior of the telephone booth. Katz was convicted based on these recordings. He challenged his conviction, arguing that the recordings were obtained in violation of his Fourth Amendment rights against unreasonable search ad seizure. The United States Supreme Court ruled in favour of Katz, holding that government wiretapping is subject to the Fourth amendment warrant requirements and physical intrusion is not necessary. Writing for the majority, Justice Stewart wrote, "[o]ne who occupies a telephone booth, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."

[34] *Katz*, *ibid* at 361. The majority opinion in *Katz* has been largely ignored. Most courts cite to Justice Harlan's concurring opinion in which the reasonable expectation of privacy test is formulated: the Fourth Amendment covers a search or seizure if (1) a person exhibits an actual or subjective expectation of privacy and (2) the expectation is one that society is prepared to recognize. In Canada, the *Katz* reasonable expectation of privacy test was expressly adopted in *Hunter*, *supra* note 22 and has since been consistently applied by the Supreme Court of Canada.

protections of spatial interests. Thus, it reasserts the relevance of spatial privacy and supports its position alongside, or better integrated with, informational privacy. It contributes by pushing us to confront, respond and adapt to pressing socio-legal concerns raised by an increasingly embedded invisible and networked society and therefore, fills a gap in privacy discourse by considering the spatial dimension of privacy, something that has largely been missing in the scholarship. Third, this dissertation makes a contribution by proposing and developing a new conceptual approach to spatial privacy. Although it was beyond the goal of this project to fit the conceptual construct into the existing legal framework, peopled places can be used as an apparatus to assist courts adapt their privacy analysis and invigorate legal protections against unreasonable search and seizures. This is important because it gives a strong conceptual foundation upon which spatial privacy may be sustained in law, the most obvious and critical next step in future work. And finally, this dissertation lays the groundwork for other interesting and important future research in two key ways: first by introducing and weaving together insights drawn from a range of perspectives that can be built upon to further inform privacy analysis; and second, the characteristics identified and forming part of the peopled places construct can be further explored as potential subsets of spatial privacy.

CHAPTER ONE

THE TECHNOLOGY LANDSCAPE

> *We live in a complex world, filled with myriad objects, tools, toys and people. Our lives are spent in diverse interaction with this environment. Yet, for the most part, our computing takes place sitting in front of, and staring at, a singling glowing screen attached to an array of buttons and a mouse. From the isolation of our workstations we try to interact with the surrounding environment, but the two worlds have little in common. How can we escape from the computer screen and bring these two worlds together?*
>
> Pierre Wellner, Wendy McKay & Rich Gold, *Back to the Real World* (1993)

1. Introduction

Walt Disney was a visionary.[1] While perhaps not the first to come to mind when considering modern computing and technology,[2] his focus on employing the latest technologies to ease and better everyday life resonate in today's world of computing. In particular, he had the idea of being able to take a physical space, a blank canvas, and transform it into something inspired; the original Disneyland. Visitors could experience living in the homes of the future, a concept Disney developed to showcase progress and what evolved to become the model city 'Tomorrowland.' It was not only Disney fantasy worlds that Disney created. He became increasingly fascinated with the idea of building 'spaces' that would make people's everyday lives less chaotic and engaged himself in creating ways to improve the way real people live together in real places.

His vision was to build a city where people would live, work and play in an environment that embraced technology. Disney's 'Carousal of Progress' show debuted

---

1 Neil Gabler, *Walt Disney: The Triumph of the American Imagination* (New York: Random House, 2006); Louise Krasniewicz and Michael Blitz, *Walt Disney: A Biography* (Santa Barbara, CA: Greenwood, 2010). See generally online: <http://www.waltdisney.org>.

2 For example, more familiar names might include computing and technology pioneers Charles Babbage, Vannevar Bush, Alan Turing, Tim Berners-Lee, Bill Gates and Steve Jobs.

at the 1964 New York World Fair which, according to its theme song "A Great Big Beautiful Tomorrow" explored the 'joys' of living through the advent of technological innovations. But it was not just about technology for Disney, it was about reinventing society.

This enduring philosophy was what Walt Disney sought to bring to urban redesign in a massive project he called the 'Experimental Prototype Community of Tomorrow' (EPCOT). This community was a carefully designed city that Disney would build from the ground up on some 50 acres of land he purchased in Orlando, Florida. EPCOT would be a 'perfect' city with dependable state-of-the-art public transportation, underground utility access tunnels, a huge soaring civic centre covered by an all-weather dome, model factory environments that would be concealed by green belts, and everything would be readily accessible to workers housed in idyllic suburban subdivisions nearby. A model for urban change, a 'city of tomorrow' with a population of 20,000, incorporating the newest technologies, constantly updated to test and discover the best way for a city to be, for people to live. Walt Disney died in 1966 and his dream of an experimental city was never realized. The EPCOT amusement park at Disneyworld that was eventually built is devoted to technology and world cultures, but bears little resemblance to the utopian city of the future Disney envisioned.

Where Hewlett-Packard's 'Cooltown'[3] is the web video-based equivalent to Disney's vision, and 'Project Oxygen'[4] is MIT's lab-based research equivalent, 'Songdo City' is Korea's real world version of Disney's Tomorrowland.[5] Situated about 60 kilometers from Seoul on 1,500 acres of landfill off the Inchon coast, Korea is building its own city of tomorrow where everything is similarly designed in a centrally planned

---

[3] Hewlett-Packard, "Cooltown", online: Hewlett-Packard <http://www.cooltown.com> See also Philips, "Vision of the Future," online: YouTube <http://www.youtube.com/watch?v=hvGb-o2Y_XO>; Samsung, "Future Life and Style", online: YouTube <http://www.youtube.com/watch?v=1nKFW-lDNK8>; and Microsoft, "Future Vision @ 2020", online: YouTube <http://www.youtube.com/watch?v=55p3vNCF4JQ>.

[4] Massachusetts Institute of Technology, "Project Oxygen", online: MIT Oxygen Project <http://oxygen.lcs.mit.edu/>. See also Carnegie Mellon University, "Project Aura", online: Aura <http://www.etc.cmu.edu/projects/aura>; and University of California Berkeley, "The Endeavour Expedition: Charting the Fluid Information Utility", online: Endeavor Project <http://endeavour.cs.berkeley.edu>.

[5] Gale International, "SongdoIBD", online: <http://www.songdo.com>.

utopian community. Expected to be completed in 2015, more than 60,000 will live and 300,000 people will work in the new Songdo City. Described as the largest test bed for technology Songdo, or 'U-City' is a place where imagination and computing technology intersect. Reminiscent of Disney's vision of an experimental city to give residents what they need to make work, play and life easier and more enjoyable, Songdo unites a community in the belief that ubiquitous technology will add value to people's lives.

In Songdo City, new technologies will be used and dispersed within everyday lives and everyday spaces. It is projected to be an international centre where people, places and things are among the privileged of the connected world, wired and wireless, a place where e-services meet the physical world, where humans are mobile, devices are 'smart' and everything has a web presence. Every street, every house, every office will be wirelessly connected to enable a ubiquitous computing "paradise" that "demonstrates the benefits of living a digital lifestyle."[6]

The range of services Songdo City offers is impressive. From the mundane, as for example, intelligent recycling bins that use RFID technology to credit recyclers' accounts; to the inspired, as for example, smart house keys to borrow city-owned bicycles, access public transportation, plug parking meters and order pizza. Video conferencing between businesses or between neighbours and wireless access to an endless supply of information from anywhere in the city is guaranteed. Features such as pressure-sensitive floors for detecting falls and summoning help, and cell phones holding your medical history through which residents can order and pay for medication. Add to all of these practical benefits; schools for your children run by Harvard University faculty, hospitals administered by Baltimore's renowned John Hopkins, homes in a garden district, boating on a Venetian canal, golf, museums and picnic areas in Songdo's 100-acre Central Park.

Songdo City will certainly be clean, modern and efficient and perhaps, the ideal environment, perhaps. But there is a catch. It is a place where everything is tracked, every action recorded, every service personalized and every transaction automated.

---

[6] *Ibid.*

Unlike 'Tomorrowland', people won't just come and visit, they will actually live and work there. The Songdo City experiment takes a physical space and transforms it into something: the ubiquitous networked society.

Chief Technologist at the Palo Alto Research Centre (PARC), Mark Weiser, like Walt Disney, was a visionary, whose professional philosophy and life interest led him to ask "What should I build next?"[7] His vision too was to construct a technology-advanced model that would enhance and ease everyday life. While most others during that period beginning in the late 1980s were focusing on microcomputers, and the emerging artificial world of virtual reality,[8] Weiser imagined a future in which computers were invisible and everywhere, a world where "[m]achines that fit the human environment instead of forcing humans to enter theirs will make using a computer as refreshing as a walk in the woods."[9] Weiser and his PARC research colleagues called their work 'ubiquitous computing'; their version of 'Tomorrowland.'

Defining ubiquitous computing has taken on a life of its own as reflected in the range of ways and technologies it is now associated with.[10] The conceptual complexity of Ubiquitous Computing is also demonstrated by its growth as a PARC research project to an independent area of study.[11] Although there appear to be several related

---

7 Mark Weiser, "The Technologist's Responsibilities and Social Change" (1995) 2:4 Computer-Mediated Communication Magazine 17. This was Weiser's last publication because, like Walt Disney, he died before his vision began to take shape.

8 Pierre Wellner, Wendy MacKay & Rich Gold, "Back to the Real World" (1993) 3:7 Communications of the Association of Computing Machinery (ACM) 24.

9 Mark Weiser, "The Computer for the 21st Century" (1991) 265:3 Scientific American 66.

10 For example, pervasive computing, mobile computing, smart phones, wearable computing, calm technology, internet protocol, invisible computing, seamless computing, wi-fi, ambient intelligence, augmented reality, mixed reality, radio-frequency identification, intelligent environments, internet-of-things, physical computing, networked objects, smart dust, things that think, global positioning system, tangible media, body aware networks, context-aware computing, cell ID, spychips, participatory panopticon, smart homes, ambient findability, geospatial web, sensing technologies, locative media, hybrid space, dynamic privacy, location surveillance, embedded cities, human-computer interaction, user-centric, situated space, and digital life.

Note also, Adam Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing* (Berkeley, CA: New Rider, 2006) decided to replace the "ugly words" of ubiquitous computing and just call it "everyware."

11 Weiser's research team at PARC began to construct the next generation of computing systems encompassed by the Human-Computer Interaction (HCI) discipline which began in 1970s, but took off after Weiser's vision was articulated in the early 1990s: Brad Myers, "A Brief History of Human-Computer Interaction Technology" (1998) 5:2 ACM Interactions 44. Ubiquitous Computing continues to be principally

labels given to ubicomp study, almost all share Weiser's goal of "activating the world."[12] It remains, however, difficult to specify exactly what is meant by the now widespread term 'ubicomp' because it is "unusual amongst technological research areas. Most areas of computing science research are defined largely by technical problems, and driven by building upon and elaborating a body of past results. Ubiquitous computing, by contrast, encompasses a wide range of disparate technological areas brought together by a focus upon a vision."[13]

This chapter examines the emerging technological landscape, what is now considered the third paradigm of computing described as the "colonization of everyday life" by computers and information technology.[14] With its vision of applying computing ability and information technology to everyday life, ubiquitous computing promises to impact our lives in profound ways and to such an extent that personal computers and even the Internet might seem primitive. Such an impact will undoubtedly have legal consequences, some easy to anticipate, others not. This dissertation considers the privacy implications of ubiquitous computing, specifically, the impact on the spatial dimensions of privacy compromised by ubiquitous computing and how to effectively sustain legal protection of these interests. In order to do so, a thorough understanding of ubiquitous computing is required.

Chapter One begins by revisiting Weiser's vision, upon which the ubicomp paradigm has been developed. The original articulations of ubiquitous computing are used as the framework for outlining the emerging computing era. The focus of this chapter is on three salient features of ubiquitous computing; physicality, invisibility and context-awareness, all of which are examined in detail. Together, these features

---

developed within the larger discipline of Computing Science, but emerged as an area of multi-disciplinary study.

[12] Gregory Abowd & Elizabeth Mynatt, "Charting Past, Present & Future Research in Ubiquitous Computing" (March 2002) 7:1 ACM Transactions on Computer-Human Interaction 29 at 32.

[13] Genevieve Bell & Paul Dourish, "Yesterday's Tomorrows: Notes on Ubiquitous Computing Dominant Vision" (2007) 11:2 Personal & Ubiquitous Computing 133. Many of the ideas generated by Mark Weiser and his PARC colleagues have come to greater prominence. This influence has been felt across industry, government, commercial and academic research: Yvonne Rogers, "The Changing Face of HCI in the Age of Ubiquitous Computing" in Andreas Holzinger & Klaus Miesenberger, eds, *HCI and Usability for e-Inclusion* (Berlin: Springer, 2009) 1.

[14] Greenfield, *Everyware, supra* note 11 at 33.

demonstrate the shift in computing from the desktop model to our everyday world and lay the foundation for examining the spatial interests we seek to protect in law. Chapter One concludes by highlighting where we are today, the trends and applications, as ubiquitous computing continues to move from vision to reality. Based on this comprehensive study, Chapter Two looks at surveillance and the privacy implications raised by ubiquitous computing.

2. Re-visiting the Vision

2.1. What is Ubiquitous Computing?

Ubiquitous computing was presented as a vision, rather than a theoretical framework for the design of future technologies. It is, however, a broad vision, drawing on the social sciences and combining Weiser's research in computing science with his colleague Lucy Suchman's anthropological research, in which she observed the way people really used technology.[15] This led to a shift in the computing research agenda that was less focused on improving the computer itself than on improving how the computer functioned within the framework of people's daily lives. Under its guiding principle, "from atoms to culture," the PARC project was aimed at technology that moves beyond the personal desktop computer into the everyday world, the arena for human activities.[16] Ultimately, by making technology an integral part of human life, in which our routine and daily environment is augmented with computational resources that provide access, information and services, the user's quality of life improves.[17]

---

[15] Lucy Suchman, *Plans and Situated Actions: The Problem of Human-Machine Communication* (Cambridge: Cambridge University Press, 1987).

[16] Mark Weiser, "The World is not a Desktop" (1994) 1:1 Interactions 7. Reflecting on bits and atoms, MIT Media Lab researcher Neil Gershenfeld said "the bits are the good stuff" referring to units of digital information because 'they consume no resources, they travel at the speed of light, we can copy them, they can disappear, we can send them around the globe and construct billion dollar companies." Contrasting them with physical objects, "the atoms are the bad stuff. They consume resources, you have to throw them away. They're old-fashioned." He concludes that the next era of computing brings the bits into the physical world: in Charles W Schmidt, "The Networked Physical World", online: RAND Corporation <http://www.smapp.rand.org/ise/ourfuture/Internet/sec4_networked.html>.

[17] Mark Weiser, John Seely-Brown & Rich Gold, "The Origins of Ubiquitous Computing Research at PARC in the late 1980s" (1999) 38:4 IBM Systems Journal 693.

Weiser defined his vision of ubiquitous computing as "the method of enhancing computer use by making many computers available throughout the physical environment, but making them effectively invisible."[18] People will be surrounded by intelligent, intuitive interfaces with networked computing functionality that would make computer devices simple to use, unobtrusive and invisible. Ubiquitous computing then endeavours to integrate information displays into the everyday physical world and augment "the nuances of the real world" with a view to "a world of fully connected devices, with cheap, wireless networks everywhere."[19] The goal, therefore, is to create a system that is pervasively and unobtrusively embedded in the environment, completely connected, intuitive, effortlessly portable and constantly available. In other words, it conceives of computers leaving their boxes and becoming physically embedded where computing is no longer a conscious, focused activity, but rather an activity that fades into the background as a calm, invisible process.[20]

Weiser colleague Rich Gold described it this way:

> Ubiquitous computing is a new metaphor in which computers are spread invisibly throughout the environment, embedded and hiding as it were, within the objects of our everyday life. Each of these computers can talk with any of the other computers much like chattering animals in a living jungle, sometimes exchanging detailed information, sometimes just noting who's around. The everyday objects themselves become a kind of ruse: a baby doll (or toy block) might look like a familiar remnant of childhood, but it is really only one of a thousand distributed nodes which control the functioning of the whole house. Likewise, the baby doll itself activates its own mechanisms, behaviours, and charms based partly on the comings and goings of its adopted (organic) family, and partly on digital discussions with other objects in the house.[21]

The metaphorical power of Gold's description resonates today in what many refer to as the "Internet of things."[22] Put most simply, it refers to inanimate objects embedded

---

[18] Mark Weiser, "Some Computer Issues for Ubiquitous Computing" (1993) 36:7 Communications of the ACM 75.

[19] Weiser, "The Computer of the 21st Century", *supra* note 9 at 78.

[20] Greenfield, *Everyware*, *supra* note 11 at 18-23

[21] Rich Gold, "This is not a Pipe" (1993) 36 Communications of the ACM 72.

[22] The term 'internet of things' was first used, or so he claims, by Kevin Ashton at a conference in 1999: Kevin Ashton, "That 'Internet of Things' Thing" (June 2009) RFID Journal, online: Radio Frequency Technology News & Features <http://www.rfidjournal.com/article/view/4986>. It is first mentioned in the literature by Neil Gershenfeld in *When Things Start to Think* (New York: Henry Holt & Co, 1999) and later popularized by Bruce Sterling in his "spime-based" view of the internet of things. A "SPIME" is a physical object trackable

with computing power that connects those objects, in both a sensory and intelligent manner, to humans and to each other. Embedding short range mobile transceivers into a wider array of gadgets and everyday items will enable new forms of communication between people and things, and between things themselves. Connections multiply and create an entirely new dynamic network of networks.[23] Central to its actualization is the ability of computers to be perceptive, interpretative and reactive. This is achieved by the integration of several enabling technologies. Key among these enabling technologies are Radio-Frequency-Identification (RFID)[24] and Wireless Sensor Networks (WSN).[25] RFID is not new, but tagging things and people is increasingly being refined and developed for current and potential use across a broad spectrum.[26] Adding

---

through space and time, which is made possible by a landscape of networked sensors and communication systems: *Shaping Things* (Cambridge, MA: MIT Press, 2005). See also, for example, keynote addresses by Bruce Sterling, "Spimes and The Future of Artifacts" (LIFT Conference, February 3, 2006), online: YouTube <http://www.youtube.com/watch?v=E2Fb7ezbVtY&feature=gv>; "The Future, The Internet and the World Wide Web" (O'Reilly Media Emerging Technology Conference, March 2006), online: ITC Conversations <http://itc.conversationsnetwork.org/shows/detail717.html>; and "The Internet of Things: What is Spime and Why is it Useful" (Google TechTalks, April 2007), online: YouTube <http://www.youtube.com/watch?v=avCLyNRbw3Q>.

Adam Greenfield's 'Everyware', *supra* note 11, is, essentially, a description of the 'internet of things.'

[23] See for example, Julian Bleecker, "Why Things Matter", online: Scribd <http://www.scribd.com/doc/14748019/Why-Things-Matter>; Neil Gershenfeld, Raffi Krikorian & Dany Cohen, "The Internet of Things" (2004) 291:4 Scientific American 76; and see generally, Council on the Internet of Things think-tank, online: The Internet of Things <http://www.theinternetofthings.eu/>.

[24] RFID is the acronym referring to small electronic devices that consist of a small chip and antenna which are embedded into things, people and places. The RFID device serves the same purpose as a bar code or a magnetic strip providing a unique identifier for that object. Put simply, individually programmed RFID tags, or transponders, use radio signals to capture and share data between mobile and fixed computing devices, allowing automatic data capture and object identification. For a detailed description, see Simson Garfinkel & Beth Rosenberg, eds, *RFID: Applications, Security and Privacy* (New Jersey: Pearson Education, 2006); and Office of the Privacy Commissioner of Canada Fact Sheet: RFID Technology, <http://www.priv.gc.ca/resource/fs-fi/02_05_d_28_e.asp>.

[25] Wireless Sensor Networks consist of spatially distributed and connected autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, humidity or motion. WSN systems typically operate by the collection and distribution of data controlled by a management centre. For a detailed description, see Kazem Sohraby, Daniel Minoli & Taieb Znati, *Wireless Sensor Networks: Technology, Protocols and Applications* (Hoboken, NJ: John Wiley & Sons, 2007).

[26] Badi Nath, Frank Reynolds & Roy Want, "RFID Technology and Applications" (2006) 5:1 IEEE Pervasive Computing 22. See also 2007 lecture by founding executive editor of *Wired Magazine*: Kevin Kelly, "Predicting the Next 5000 Days of the Web", online: YouTube <http://www.youtube.com/watch?v=yDYCf4ONh5M>, in which he argued that in the first 5000 days of the world wide web, "less time than it takes for a child to progress through the school system, the world had been transformed" and in the next 5000 days of the web, the speed in which the web has caught on and the haste with which it has transformed the industrialized world showed no signs of slowing, to the point that "[e]verything will be part of the web. Every item, every artefact will have some sliver of connectivity that will be part of the web." In other words, according to Kelly in 2007, everything will be connected to

sensor technology gives the eyes and ears access to a networked system. The convergence of enabling technologies, particularly as they become cheaper, smaller and more powerful, takes us closer to the world envisioned by Weiser.

2.2. Salient Features of Ubiquitous Computing

2.2.1 Physicality

For Weiser, "making computers available throughout the physical environment" meant bringing technologies into the real world in which human activities and interactions occur.[27] Ubicomp then takes as its starting point that "the everyday world is the arena for human activities that we should design for."[28] Ubicomp, therefore, challenged not only the 'desktop' computer machinery, but also the virtual reality paradigm, thus positioning itself as an alternative. While virtual reality was trying to immerse people in a computer-generated world, thereby leaving the everyday physical world behind, ubicomp took a very different approach and aimed for technology to become an integral part of human activities as they occur in our everyday physical environment.[29]

Ubiquitous computing will be everywhere. This is its essence, its explicit goal.[30] The seamless integration of computing intended to populate the physical world by residing in everyday objects, environments and even ourselves.[31] Once combined,

---

the point where "the environment will become the web." What Kelly was describing was an 'internet of things,' namely, a world where a pair of shoes becomes seen as "a chip with heels; a car as a chip with wheels." It is a network of connected objects. Vehicles, domestic consumables, the clothes on your back, all being hooked up to a network with a speed most of us have yet to comprehend.

27 Weiser, "The Computer of the 21st Century", *supra* note 9 at 80.

28 Weiser, "Some Computer Issues in Ubiquitous Computing" *supra* note 20 at 75.

29 *Ibid*.

30 Greenfield, *Everyware, supra* note 11.

31 On human chip implants, see for example, Rodney Ip, Katina Michael & M G Michael, "Toward Chipification: The Multifunctional Body," online: University of Wollongong, Faculty of Informatics <http://ro.uow.edu.au/infopapers/372/>; Rodney Ip, Katrina Michael & M G Michael, "The Social Implications of Human-centric Chip Implants: Thy Chipdom Come, Thy Will Be Done," online: University of Wollongong, Faculty of Informatics <http://ro.uow.edu.au/infopapers/601/>; Ian Kerr, "The Internet of People: Reflections on the Future Regulation of Human-Implantable Radio-Frequency Identification" in Ian

integrated and connected, a massive geo-web is created, affecting most, if not every, space and activity in our daily lives; from crossing the street to sitting in your living room to entering an office building. Therefore, physicality refers not only to the spatially embedded nature of our environment, but also to the physical objects or artifacts we use in our everyday lives.

Malcolm McCullough argues that computing technologies are increasingly pervading the built environment. In his view, previous paradigms in cyberspace threatened to de-materialize architecture, but ubiquitous computing invites a defense of architecture because it is grounded in the legacy of architectural design theory.[32] No matter how much a technological innovation purports to make the built environment ephemeral, we cannot escape the fundamentals of architecture.[33] In sum, his essential claim is that architects and technologist designers "must now serve our basic human need for getting into place."[34] Therefore, within the context of ubiquitous technologies, which weave themselves into the fabric of built environments, architectural design informs interaction design as much as interaction design transforms architectural design.[35]

What all of this means – and it is significant – is first, that geography matters, and second, that 'cyberspace' may matter less. In fact, geography may matter more. The Internet undermined the significance of physical space, at least in terms of location and distance, but the ubiquitous computing 'anywhere' paradigm makes physical space and location relevant again. The physically embedded nature of ubiquitous computing directly penetrates physical space, the space in which real people live, work, interact and move. This means all spaces, including those which are conventionally understood as private and public spaces.

Kerr, Valerie Steeves & Carole Lucock, eds, *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked* Society (Toronto, ON: Oxford University Press, 2009) 335.

[32] Malcolm McCullough, *Digital Ground* (Cambridge, MA: MIT Press, 2005) ix.

[33] *Ibid* at 9.

[34] *Ibid* at xiv.

[35] *Ibid* at 19.

Regardless of how one might characterize 'cyberspace,'[36] you can walk away from the computer screen, but ubicomp surrounds us and concerns itself with an individual's location and the location of the environment in which ubicomp is embedded. For example, via global positioning satellite technology, as you enter Costco your friends in the same store can be notified that you are headed towards the hot dog stand, or as you near a particular highway exit, your location will determine what restaurant chain's advertisement you receive.

While these simple examples may seem to emphasize personalization rather than location, with ubicomp the personalization is not only with respect to the individual, but also to the physical environment in which the technology is embedded. Also, different physical environments, at different locations, will have widely different types of computing embedded, thereby subjecting people to heterogeneous computing environments.[37] For example, an airport is likely to have qualitatively different tracking infrastructures than a friend's home. But at the other extreme, there may be spots, as for example, locations or places while on vacation that are specifically designed with minimal ubicomp for those who do not want to 'stay in touch' or social clubs, which might employ RFID blockers to promote anonymity while providing access to other information, such as availability or sexual preferences. And, even within the same general physical environment, such as a university campus, ubiquitous computing may operate in ways that are unique to the place of embedding. For example, specific locations on campus may be subject to greater security than others.[38]

---

[36] See for example, William Gibson, *Neuromancer* (New York: Ace Books, 1984); John Perry Barlow, "A Declaration of the Independence of Cyberspace", online: Electronic Frontier Foundation <http://projects.eff.org/~barlow/Declaration-Final.html>; David R Johnston & David G Post, "Law and Borders: The Rise of Cyberspace" (1996) 48 Stan L Rev 1367; Dan Hunter, "Cyberspace as Place and the Tragedy of the Digital Anticommons" (2003) 91:2 Calif L Rev 439; and Julie Cohen, "Cyberspace as/and Space" (2007) 107 Colum L Rev 210.

[37] Vassilis Kostakos & Eamonn O'Neill, "A Space-oriented Approach to Designing Pervasive Systems", online: University of Bath, Department of Computer Science <http://www.cs.bath.ac.uk/pervasive/publications/ukubinet05.pdf>; Marc Auge, *Non-Places: Introduction to an Anthropology of Supermodernity* (New York: Verso, 1995); and Xiang Song, *Seamless Mobility in the Ubiquitous Computing Environment* (Ann Arbor, MI: ProQuest, 2008).

[38] Louise Barkhaus & Paul Dourish, "Everyday Encounters with Context-Aware Computing in the Campus Environment" in *Proceedings of the International Conference on Ubiquitous Computing* (Nottingham, UK: Springer, 2004) 232.

Thus, the locations in physical space and places of activity and interaction matter, affecting not just the information that may be gathered or accessed, but also the ways in which technology becomes an omnipresent part of our physical existence within and across those spaces and places.

What emerges from the concomitant roles of physicality and spatiality within Weiser's vision are several related and important aspects; mobility, augmented reality, hybridization and embodied interaction. Each are critical to furthering our understanding of how computing is being brought back into the real world. Together they serve to help realize the core tenets of ubiquitous computing, and ultimately, contribute to the paradigmatic shift, not only in computing, but also in society. A shift to a world that is more physically and spatially aware, thus reinforcing the need to consider the territorial model of privacy. The remainder of this section on physicality examines these aspects.

Mobility

When you stop and think about it, mobility is central to what it is to be human. Moving your hand, walking, driving to work, moving away, and moving home again, going on a trip, attending conferences, dancing and even a job promotion are all forms of mobility. In this sense, it has been described as "a kind of blank space that stands as an alternative to place, boundedness, foundations, and stability,"[39] thus reinforcing mobility as the ability to physically move about. People obviously do not exist and live primarily in fixed locations, but rather move in their personal, professional and social spheres. Mobile computing is "fundamentally about increasing our capacity to physically move computing services with us. As a result, the computer becomes a taken-for-granted, ever present device that expands our capabilities to inscribe, remember, communicate and reason independently of the device's location."[40] To achieve Weiser's goal of ubiquitous computing, mobility is required, which he

---

[39] Tim Cresswell, *On The Move: Mobility in the Modern Western World* (New York: Routledge, 2006) 2.

[40] Kalle Lyytinen & Youngjin Yoo, "Issues and Challenges in Ubiquitous Computing" (2002) 45 Comm ACM 63.

recognized as being made possible through wireless communication technologies.[41] Thus, developing a mobile infrastructure for wireless networking was a particular focus of PARC's research agenda.

Mobility in the context of ubiquitous computing can take three forms. First, computers become increasingly mobile, such that we take them with us wherever we go. This is consistent with the historical trend towards progressively smaller and more mobile computing devices; from huge mainframes, to desktops, to laptops, to PDAs, to cell phones.[42] Second, ubiquitous computing mobility refers to always having access to computing ability and access to one's data through broadband-networked computers embedded throughout the physical environment.[43] In other words, with mobility, computing services move with us. Thus, personal data, preferences and services would not exist on multiple devices with different settings, but would be available seamlessly to us anywhere and at any time. Third, the mobile system is capable of functioning autonomously and through user control.[44] These new kinds of machines, "are autonomous or semi-autonomous: they create their own assessments, make their own decisions. They no longer need people to authorize their actions."[45] For example, a ubiquitous computing environment could automatically sense your presence and carry out certain functions, such as adjusting thermostat settings to meet your stored preferences, notifying friends of your present location, re-routing communication attempts to your present location or rescheduling appointments that the computer determines you will not be able to make based on your current location.

The ubiquitous computing society, therefore, will be organized around new 'machines' which enable people to be more individually mobile through space, forming connections on the go. People will "occur as various nodes in multiple machines of inhabitation and mobility. Through inhabiting, or internalizing, such machines come to

---

41 Weiser, "The Computer of the 21st Century", *supra* note 9 at 86-87.

42 Lyytinen & Yoo, *supra* note 42 at 64.

43 *Ibid.*

44 Johanna Brewer & Paul Dourish, "Mobility, Technology and Environmental Knowing" (2008) Intl J of HCI; Maso Kakihara & Carsten Sorenson, "Expanding the Mobility Concept" (2001) 22:3 Comm ACM 33.

45 Donald Norman, *The Design of Future Things* (New York: Basic Books, 2007) 36.

life."[46] The 'machines' are increasingly becoming smaller, digitized and mobilized, including not just mobile phones, iPods, tablets and laptops, but also everyday moving things such as cars, bikes or aircrafts. In addition to the increasing diversity of mobile devices is the trend toward a seamless convergence of devices.[47] While the technologies may differ, they are united in a common philosophy, "the primacy of the physical world and the construction of appropriate tools that enhance our daily activities."[48]

A key feature emerging from the new mobility paradigm is location-awareness. With today's mobile devices, not only can we connect to the Internet anywhere at any time, we can also map our precise geographic coordinates and access location-specific information that enables us to engage with our surroundings. The mobile technologies we use to access the Internet are location-aware, linking digital data to a specific place. Location-aware technologies are mobile devices able to locate themselves via global positioning system (GPS), Wi-Fi, RFID, or sensor networks and are, therefore, able to provide users with location-specific information. In other words, location-aware technology delivers information about a device's physical location to another user or application. Location-aware technologies strengthen people's connections to their surroundings because they help users to locate other people and things around them in the physical world.

Weiser's idea of ubicomp was, among other things, based on location-awareness. PARC's prototypes, such as the PARCTab, the PARCPad and the Live Board,

---

[46] Mimi Sheller & John Urry, "The New Mobilities Paradigm" (2006) 38:2 Environment & Planning A 207 at 221.

[47] As we acquire more devices, we also have devices that combine functions formerly performed by different technologies. For example, smart phones, android phones and the iPhone now feature voice calling, web browsing, music storage, relatively good cameras, advanced gaming, near-field communication systems that allow them to act as credit cards and Kindle applications that let people read books on their phones. The same is true of new tablet computers that combine the functionality of multiple devices inside a single device. See also, for example, ITU Report, "Mobile Technologies: Towards a Converged World" (2004), online: International Telecommunication Union <http://itu.int/osg/spu/ni/futuremobile/broadbandmobile.pdf>; video, "Convergence of Mobile Devices in the Physical World", online: YouTube <http://www.youtube.com/watch?v=6cnFwxTI4eQ>; and Henry Jenkins*, Convergence Culture* (New York: New York University Press, 2005).

[48] Pierre Wellner, Wendy MacKay & Rich Gold, "Computer-Augmented Environments: Back to the Real World" (1993) Comm ACM 26.

tracked the position of PARC employees and transmitted it to a central server in order to provide them with location-based information. They were designed to be used inside an office space because connectivity in closed spaces was easy to obtain, but as soon as wireless positioning systems started to colonize physical spaces and location could be obtained beyond closed spaces, ubiquitous computing moved outdoors. Most of the emerging mobile technologies today include some kind of location-awareness. Smartphones include GPS technology.[49] Most iPads and Kindles connect to the internet via Wi-Fi and some iPod models include Wi-Fi. RFID tags are embedded in the things we wear and use, rendering them locatable through sensor technology. And insofar as technologies have a wireless connection, they can be located and are location-aware, thus extending the Internet to physical locations.

Augmented Reality

The 1990s gave us cyberspace,[50] "a nebulous domain that exists somewhere beyond our computer screens."[51] Precisely what Weiser was "diametrically opposed" to in his vision of ubiquitous computing.[52] Unlike virtual reality, which replaces the real world with a simulated one, augmented reality is a view of a physical real-world environment whose elements are augmented by computer-generated sensory input such as sound, graphics or GPS.[53] While Weiser did not use the term 'augmented reality,' an important aspect of ubiquitous computing is to enhance people and the

---

[49] Since 2008, the release of the GPS-enabled iPhone 3G, Google's Android operating system and other 'smart phones' has contributed to the popularization and commercialization of location-aware applications, or location-based service (LBS), moving these applications into the mainstream. There are currently a wide variety of LBSs including applications, for example, that show users the closest bank machine or provide reviews of all the restaurants in the users' physical proximity.

[50] William Gibson is perhaps best known for introducing the word 'cyberspace' in *Burning Chrome* (New York, NY: Harper Collins, 1986) and describing the future global computer network as "consensual hallucination" in *Neuromancer*, *supra* note 38 at 67.

[51] Eric Kabisch, "Datascape: A Synthesis of Digital and Embodied Worlds" (2008) 11:3 Space and Culture 222.

[52] Weiser, "The Computer of the 21st Century", *supra* note 9 at 78.

[53] Wellner, McKay & Gold, "Computer-Augmented Environments: Back to the Real World", *supra* note 50; Wendy McKay, "Augmented Reality: Linking the Real and Virtual Worlds, a New Paradigm for Interacting with Computers" in Tiziana Catarei et al, eds, *Proceedings of the Working Conference on Advanced Visual Interfaces* (New York: ACM, 1998); Rolf Hainich, *The End of Hardware: A Novel Approach to Augmented Reality*, 3rd ed, (Charleston, SC: Booksurge, 2006); and Stephen Cawood & Mark Fiala, *Augmented Reality: A Practical Guide* (Raleigh, NC: Pragmatic Bookshelf, 2008).

physical environment with sensory, communicative and processing powers.[54] The ubiquitous computing paradigm differs, therefore, from virtual reality in that the orientation is to support activities in the real world. What then does this mean for 'cyberspace'? Even the word 'cyberspace' now seems somehow dated,[55] when thought of as dematerialized space, having no physicality, no matter, and no Cartesian aspect. The distinction between real space and cyberspace seems much less applicable, especially when you consider that the goal of ubicomp was never an ever-more realistic virtual reality where we immerse ourselves into a copy of the real world constructed on a computer server.

Paradoxically, the very same seminal articles by Weiser that seemingly pit virtual reality against ubiquitous computing hint at a relationship between the two that is far more complicated than one of simple opposition. Weiser's "embodied virtuality" emphasizes the differences between ubiquitous computing and virtual reality, but it also highlights the similarity between the two because both are computer mediated. In fact, a virtual world is completely computer mediated which is effectively what ubiquitous computing does, with computing ability permeating every aspect of life. Moreover, the term 'embodied virtuality' suggests that it is not the value of virtuality itself that is being disputed by the new paradigm of ubiquitous computing, but rather what is being disputed is the idea that virtuality belongs only to simulated environments. Indeed, Weiser admits that computing is always already virtual. Thus, it is impossible to imagine a pure and complete separation from, and return to, the 'real world' that is not marked by virtual experience.

Manuel Castells argues that ubiquitous digital media and network technologies are ushering in a new, more physical mode of virtual experience, adopting "real virtuality" to describe this new, non-simulated environment.[56] An environment that is interactive, that is, spaces and things that are responsive to users. Similarly,

---

[54] Mark Weiser, The Computer for the 21st Century", *supra* note 9 and "Computing Science Issues for Ubiquitous Computing" (1999) 3:3 Mob Comp and Comm Rev 12.

[55] Malcolm McCullough, "On the Urbanism of Locative Media" (2006) 18:2 Places 26.

[56] Manuel Castells, *The Rise of the Network Society* (Cambridge, MA: Blackwell, 1996) 372-373.

responsiveness is a key term in ubiquitous computing, one which PARC first started talking about in its earliest publications when creating "responsive environments" and "responsive objects."[57] The paradigm shift of ubiquitous computing, therefore, is not really an escape from virtuality, but rather a movement toward a more materially-based virtuality. In this way, it is not the end of cyberspace, per se, but reinforces the salience of physicality in the ubiquitous computing paradigm.

By augmenting real spaces, places and things with virtual reality, "the information age, or 'the network society' is not some immaterial or anti-geographical stampede online."[58] Rather, the embeddedness and animated features of ubicomp act like a "digital nervous system"[59] grafted into the physical environment in which it responds, without human intervention, to the sensed circumstances. Not only is the surrounding environment responsive and communicative, but the individual's personal space is, itself, endowed with added capabilities. In effect, augmented capabilities of and between spaces/places, objects and the body become the spatial and material embodiment of ubiquitous computing.[60] Thus transforming our ideas and expectations about space because the extension and negotiation of boundaries, previously made clearer by physical barriers, clothing and skin, become more complex. The complexity is compounded by the intermixing of the virtual and physical worlds.

Hybridization

Traditionally, physical space and virtual space are considered separate and distinct. Users in each space operate within the scope of that space. They may

---

[57] Mark Weiser, "The Computer of the 21st Century", *supra* note 9 and "The World is Not a Desktop", *supra* note 18.

[58] Stephen Graham, "Excavating the Material Geographies of Cyber-cities" in Stephen Graham, ed, *The Cyber-cities Reader* (London: Routledge, 2003) 139.

[59] This metaphor originated with Marshall McLuhan, *Gutenberg Galaxy: The Making of a Topographic Man* (Toronto, ON: University of Toronto Press, 1962). Bill Gates began using it in *Business at The Speed of Thought: Using a Digital Nervous System* (New York: Warner Books, 1999).

[60] Amanda Williams, Eric Kabisch & Paul Dourish, "From Interaction to Participation: Configuring Space Through Embodied Interaction" in Michael Beigl, Stephen Intille, Jun Rekimoto & Hideyuk Tokuda, *Lecture Notes in Computing Science: Ubicomp 2005* (Berlin: Springer, 2005) 287; Anne Galloway, "Imitations of Everyday Life: Ubiquitous Computing and the City" (2004) 18:2-3 Cultural Studies 384. Julie Cohen described "embodied space" as "the spaces of the body" in "Cyberspace as/and Space," *supra* note 38 at 33.

communicate among themselves, but do not cross the boundary into the other space. However, as ubiquitous computing becomes more pervasive in everyday life, we will live simultaneously in physical space and virtual space.[61] This dual existence, produced by the wider convergence of physical and virtual environments has been characterized as 'hybridization,' or a type of new postmodern space referred to as "hybrid space."[62] It is, in essence, a "virtual layer of digital information and interaction opportunities that sit on top of and augment the physical environment."[63] While the physical space is virtually enhanced with information, the virtual space is continuously refreshed with real-time, real-world information.

Hybridization is being driven by two distinct yet overlapping trends: connectivity and mobility. The possibility of being always connected to a network means we are literally carrying the Internet wherever we go. Because ubicomp devices are constantly connected to the Internet, you do not perceive physical and virtual spaces as separate and do not have the feeling of 'entering' the Internet, or being immersed in cyberspace, as is generally the case when you need to sit down in front of a computer screen and log on. This is precisely what Weiser was attempting to achieve in modeling an off-the-desktop paradigm. Without the sharp distinction between real space and cyberspace, hybrid space occurs when you no longer need to go out of physical space per se to get in touch, or connect with virtual environments. Rather, the

---

61 Howard Rheingold, *Smart Mobs: The Next Social Revolution* (Cambridge, MA: Perseus, 2002); Amanda Mitra & Rae Lynn Schwartz, "From Cyberspace to Cybernetic Space: Rethinking the Relationship Between Real and Virtual Spaces" (2001) 1 JCMC 7; Chin Ooi, Kian Lee Tam & Anthony Tung, "Sense the Physical, Walk Through the Virtual, Manage the Co (existing) Spaces: A Database Perspective" (2009) 38:3 SIGMOD Record 5.

62 Eric Kabisch, "Datascape: From Virtual to Hybrid Worlds", *supra* note 51; Adriana de Souza e Silva, "From Cyber to Hybrid: Mobile Technologies as Interfaces of Hybrid Spaces" (2006) 9:3 Space and Culture 261; Andy Crabtree & Tom Rodden, "Hybrid Ecologies: Understanding Co-operative Interaction in Emerging Physical-Digital Environments" (2008) 12:7 Personal & Ubiquitous Computing 481. Other terms have been used representing essentially the same concept or variations on the same idea of merging physical and virtual worlds: for example, "augmented space" used in Lev Manovich, "The Poetics of Augmented Space" (2002) 5:2 Vis. Comm. 219; "enacted space" in Gregory Pottie & William Kaiser, *Principles of Embedded Networked System Design* (Cambridge, UK: Cambridge University Press, 2005); and "symbiotic space" in Bruce Sterling, *Shaping Things* (Cambridge, MA: MIT Press, 2005).

63 Mark Bilandzic, "The Embodied Hybrid Space: Designing Ubiquitous Computing Towards an Amplification of Situated Real World Experiences" in *Proceedings of OZCHI* (New York: ACM, 2010) 422.

ubicomp environment embodies virtuality in an array of wireless devices that embed computing in the physical world.[64]

If cyberspace is somewhere people go, then hybrid space is increasingly where people are. Therefore, the borders between virtual and physical spaces, which were apparently clear with the fixed Internet, become blurred and no longer clearly distinguishable. And if the line between private and public zones has over the years already been weakened by technology, living in a hybrid world, or world of hybrid spaces, potentially dissolves it altogether. William Gibson, originator of the term cyberspace, has now acknowledged that "[o]ne of the things our grandchildren will find quaintest about us is that we distinguish the digital from the real, the virtual from the real. In the future, that will become literally impossible."[65]

The second driving factor contributing to hybridization is mobility. As discussed earlier in this chapter, today, people are increasingly on the move, in large part because they can communicate and be connected without being at a fixed location. We move from one sphere of our lives to another and within each sphere, move from one activity or place to another, as captured by Manuel Castell's "space of flows." [66] Within these flows, there are spheres of mobility[67] across which motion today is an integral part of everyday life, and are now more concretely within ubicomp's spatial reach.[68]

Ubiquitous computing throughout the physical environment means it has an inherently different physical form beyond the desktop computing model. Instead of a

---

64 Crabtree & Rodden, "Hybrid Ecologies", *supra* note 64; Weiser, "The Computer of the 21st Century," *supra* note 9.

65 *Rolling Stone* interview with William Gibson, online: Rolling Stone <http://www.rollingstone.com/politics/story/17227831/william_gibson_the_rolling_stone_40th_anniversary_interview>.

66 The "space of flows" refers to social practices in the material world applied to the digital society: Castells, *The Rise of the Networked Society, supra* note 58.

67 These spheres refer to private, public and built spaces: Colin Bennett & Priscilla Reagan, "Surveillance & Mobilities" (2004) 1:4 Surveillance and Society 451.

68 See for example, McCullough, *Digital Ground*, *supra* note 34; Mathew Honan, "I Am Here" *Wired* (February 2009), online: Wired <www.wired.com/gadgets/wireless/magazine/17-02/lp_guineapig>; Vassilis Kostakos et al, "Design Tools for Pervasive Computing in Urban Environments" in *Proceedings 8th International Conference on Design and Decision Support Systems in Architecture and Urban Planning* (Netherlands: Springer, 2006) 467; and Michael Fox & Miles Kemp, *Interactive Architecture* (New York: Princeton Architectural Press, 2010).

fixed or static space or place for computing interaction, ubiquitous computing occupies multiple spatially distributed spaces and places for interaction between people and technology. Clearly, people can and do take their computing devices with them and use them in many physical and social scenarios. By extension, this means moving from temporally isolated encounters between people and technology towards technology that is continually present and always on. It is portable, it goes wherever we go or is 'there' wherever we go in real time. In this way, it is not just 'a' location that is implicated, but also our movement across all the spaces of our everyday lives. In other words, it extends beyond clearly defined, often bounded, places to any space we move in. Therefore, mobility, the constant movement of users who interact with a conglomeration of portable objects and devices that are capable of wireless networking, is contributing to hybridization.

The shift from sedentary to mobile internet access is not a minor point. When mobility and digital information merge, the nature of the information changes. For example, this shift can be seen in the development of location-based services (LBSs). LBSs began to gain prominence with the release of the iPhone in 2007 and they take advantage of the mobile phone's internet connection and GPS technology. These services locate users in physical space and provide information about that space. LBSs include a wide range of applications, ranging from applications that map Wikipedia articles about users' surrounding spaces to Location-Based-Social-Networks (LBSNs) that map the position of the members of users' social networks. As mobile individuals access digital information that is mapped onto physical space, the nature of both the digital and the physical changes.[69] The information becomes part of that space and the interface of the mobile device becomes a representation individuals use to negotiate their interactions with physical space.

---

[69] Hiroshi Ishii, "Tangible Bits: Coupling Physicality and Virtuality Through Tangible User Interfaces" in Yuichi Ohta &Hideyuki Tamura, eds, *Mixed Reality: Merging Real and Virtual Worlds* (New York: Springer, 1999) 229.

Increasingly, our everyday lives "are being governed by the three-dimensional model of space."[70] These dimensions, or layers, are built by "the mix of social practices that occur simultaneously in digital and physical spaces, together with mobility, that creates the concept of hybrid reality."[71] It is then not only by the spatial context of the built environment in which we move from place to place, but also by social practices and the technology-enhanced interaction of the people within that physical environment.[72] Spaces and places, as physical settings for social conduct, action and interaction, seem to be an obvious, yet neglected, fundamental aspect of how ubicomp systems operate. Not only are technologies changing in terms of their computational capabilities, appearance, physical arrangement, perception and use, but also in terms of everyday social settings, by providing functionalities that impact on features of the space we occupy and where human activities occur. Embedded ubicomp devices and systems that wirelessly engage and link people and things both exploit social interaction and practices in the physical world, creating hybrid spaces. [73] This is not unlike what Julie Cohen describes as "embodied networked space" depicting a new sense of social space,[74] or Manuel Castell's "space of flows as a new spatial form characteristic of social practices that dominate and shape the network society."[75]

For the notion of hybrid space then, space is a concept produced and embedded by social practices in which the support infrastructure is composed of a network of mobile technologies. Because social spaces are not material things, but rather a set of social relationships both between objects and objects and people and objects, the logic of hybrid spaces mediates this set of relationships of ubicomp technologies.[76] The

---

[70] Sam Kingsley, "Cellspace: The Prototype for a New Society", online: SamKinsley.com <www.samkinsley.com/archives/000019.html>.

[71] de Souza e Silva*, supra* note 64 at 265.

[72] *Ibid*.

[73] *Ibid*; Kabisch, *supra* note 53.

[74] Cohen, "Cyberspace as/and Space", *supra* note 38.

[75] Castells, *supra* note 58 at 453.

[76] Henri Lefebvre, *The Production of Space* (Oxford, UK: Blackwell, 1991) 83; Felix Stadler "The Space of Flows: Notes on the Emergence, Characteristics and Possible Impact on Physical Space" (13 February 2006) online: Notes and Nodes <http://felix.openflows.com/html/space_of_flows.html>.

connections do not occur solely in physical space, but rather in a new type of space that merges physical and virtual.

This is consistent with Weiser's ubiquitous computing model, because central to this vision is that computational systems are not used in isolation, but take part in a complex interplay between people, tasks, physical objects and technology. For Weiser, "the unit of design should be social people, in their environment, plus your device."[77] PARC's new direction "recognizes even more that people are social creatures… ubicomp honours the complexity of human relationships, the fact that we have bodies, are mobile."[78] This means that technologies are embedded in the physical world, but also implicitly capture computing in the social environment. As physical beings, we are unavoidably enmeshed in a world of physical facts and things. We cannot escape the world of physical objects that we sit on, lift, move, and carry, nor the consequences of physical phenomena such as gravity and inertia. At the same time, we interact daily with other people and we live in a world that is socially constructed.[79] Elements of our daily experience – children, friends, family, technology, roads, stores, and work – gain their meaning from our interactions with them. Thus, the physical and the social are intertwined and inescapable aspects of our everyday lives. Ubiquitous computing, as envisioned by Weiser, is an attempt to capitalize on these everyday experiences and our familiarity with them.

Embodied Interaction

The current paradigm of human-computer interaction still consists mostly of standard computer interaction techniques such as keyboards and mouse devices which have been around for decades. As well, the discourse on this type of screen technology and computing has been dominated by metaphors that describe the immersive effects

---

[77] Mark Weiser, "User Interface, Systems, and Technologies" ACM keynote address (November, 1994), slides online: <http://www.ubiq.com/hypertext/weiser/UbiHome.html

[78] Mark Weiser quoted in Howard Rheingold, "PARC is Back" *Wired* (February, 1994), online: Wired <http://www.wired.com/wired/archive/2.02/parc_pr.html>.

[79] For a detailed discussion on the concept of 'socially constructed space' see Lefebvre, *The Production of Space, supra* note 78.

of virtual space. Concepts such as the "virtual gaze"[80] and "armchair traveler"[81] underscore the idea of a Cartesian subject with a mind/body dualism engaged with a machine. In other words, a person disembodied from the physical world "using an application or tool, or as a communication process between human and machine."[82] This approach overlooks, as philosopher Martin Heidegger posits, the sense of 'being' and the ways that we encounter the world and act through it to define meaning and action.[83] This is implicit in Weiser's vision of bringing the interaction between humans and computers closer together through more natural and embodied interaction with the digital environment around us. As ubiquitous computing evolves, interaction is being seen less as interaction with standard computer systems alone, as for example desktop environments, and more as interaction with everyday objects.[84] In this way, ubiquitous computing plays an important role in reducing the borders between humans and computers in order to make interactive systems embodied in the real world environment.

The notion of embodiment is not a new one, but has been a common theme throughout philosophy, cognitive science, and is at the centre of a branch of philosophy called phenomenology, which is principally concerned with the elements of the human experience.[85] From this perspective, humans are seen as embodied beings with

---

[80] Anne Friedberg, "The Mobilized and the Virtual Gaze in Modernity" in Nicholas Mirzoeff, ed, *The Visual Culture Reader* (New York: Routledge, 2002) 395.

[81] Erkki Huhtamo, "Armchair Traveller and the Virtual Voyager" (1995) 6:2-3 Mediamatic 13.

[82] Francis Quek, "Embodiment and Multimodality" in *Proceedings of ICMI 2006 International Conference on Multimodal Interfaces* (New York: ACM Press, 2006) 388.

[83] Martin Heidegger, *Being and Time*, translated by John MacQuarrie & Edward Robinson (New York: Harper and Row, 1962). Weiser cites Heidegger in his first article about ubiquitous computing: "The Computer for the 21st Century" *supra* note 9.

[84] Scott Klemmer, "Integrating Physical and Digital Interactions" (2005) Computer 111; John McCarthy, Peter Wright, Jane Wallace & Andy Deardon, "The Experience of Enchantment in Human-Computer Interaction" (2006) 10:6 Personal and Ubiquitous Computing 369.

[85] Dermot Moran & Timothy Mooney, eds, *The Phenomenology Reader* (New York: Routledge, 2002); Shawn Gallager & Dan Zahavi, eds, *Phenomenology and the Cognitive Science* (New York: Springer, 2010).

Phenomenological theorists, Edmund Husserl, Martin Heidegger and Maurice Merleau-Ponty have been particularly relevant to questions of embodiment and interaction. Edmund Husserl was first to move away from the previous philosophical traditions and begin the attempts to reorient Cartesian thinking around human experience and human understanding, looking at how our understanding of the world was based in everyday embodied experience rather than abstract thinking. The idealized scientific conception of the world, according to Husserl, had distanced science and mathematics from the everyday world and

sensory, perceptual and cognitive abilities that are "inextricably tied to our physical being, and the need for that being to function as it is situated in a dynamic, time-pressured world."[86] Phenomenologists point out that the world is already filled with meaning, arising from the way in which the world is organized relative to our needs and actions, not just physically, but socially and historically. Thus, from the phenomenologist perspective, we encounter, interpret and sustain meaning through our embodied actions with the world and with each other. In other words, phenomenologists explore the relationship between embodied action and meaning, the source of which is not a collection of abstract, idealized entities, but rather found in the world in which we act and experience.

---

everyday practical concerns, and in doing so, had distanced it from the live experience of people acting in the world. Rather than abstract and formalized reasoning, Husserl envisioned a science that was firmly grounded on the phenomena of experience, which in turn meant developing the philosophy of experience as a rigorous science: Edmund Husserl, *Ideas: General Introduction to Pure Phenomenology,* translated by W R Boyce Gibson (New York: Routledge, 2012). See also Francisco Varela, Evan Thompson & Eleanor Rosch, *The Embodied Mind* (Cambridge, MA: MIT Press, 1991).

Martin Heidegger moved the site of that experience *into* the world, claiming embodied action was essential to our mode of being and to the ways in which we encountered the world. For Heidegger, the nature of being, how we exist in the world, shapes the way we understand the world because our understanding of the world is essentially an understanding of how we are in it. He rejected the dualism of mind and body arguing that thinking and being are fundamentally intertwined. From his perspective, the meaningfulness of everyday experience lies not in the head, but in the world. Instead of asking, "[h]ow can we know about the world?" Heidegger would ask, "[h]ow does the world reveal itself to us through our encounters with it?": Martin Heidgger, *Being and Time, supra* note 85.

Maurice Merleau-Ponty emphasized the critical role of the body in mediating between internal and external experience. Maurice Merleau-Ponty's focus was on the role of the body in perception. Perception of an external reality comes about through and in relation to a sense of the body: "All knowledge takes its place within the horizons opened up by perception" (at 241) and "if it is true that I am conscious of my body via the world…it is true for the same reason that my body is the pivot of the world…I am conscious of the world through the medium of my body." (at 94-95) Thus, for Merleau-Ponty, any theory of embodiment is ultimately a theory of the sensory because our knowledge of the world and our place within the world depends on the feedback from our senses: Maurice Merleau-Ponty, *The Phenomenology of Perception*, translated by Colin Smith (New York: Routledge Press, 1958).

The work of psychologist JJ Gibson, especially as explored by technologist Donald Norman, extended these themes to focus on interaction: *The Ecological Approach to Visual Perception* (New York: Houghton-Mifflin, 1979). Gibson recognized the importance of our physical embodiment in the world as a central aspect of how we act and react. His starting point was to consider visual perception as a point of contact between the creature and its environment, an environment in which the creature moves around and within which it acts (at 222). By placing visual perception within a frame of being and acting, Gibson laid the foundations for what he came to call "ecological psychology." In contrast to approaches such as cognitive psychology which focused on mental processing, ecological psychology studied the organism living and acting in the world, what might be described as "knowledge in the world" rather than "knowledge in the head." Gibson's work also laid a foundation for understanding human-environment interfaces: Malcolm McCullough, *Digital Ground*, *supra* note 34 at 35.

[86] Quek, *supra* note 84 at 389.

As computation becomes embedded in everyday objects and physical environments, the ideas of embodiment provide a different perspective than a Cartesian or information processing perspective on interaction. An embodied view of computing was popularized in the human-computer interaction field by Paul Dourish, who used the term "embodied interaction" to describe an approach to interaction use and design that places an emphasis on understanding and incorporating our relationship with the world around us, both physical and social.[87] Embodied interaction "is interaction with computer systems that occupy our world, a world of physical and social reality, and that exploit this fact in how they interact with us."[88] An interactive device that takes advantage of embodied interaction principles takes advantage of how people actually interact with their real-world surroundings. Understanding human-computer interaction that seeks to investigate and support this complex interplay of mind, body and environment has increasingly become an important research direction within human-computer interaction.[89]

To conclude this section on 'physicality,' early predictions of the Internet imagined that individuals would begin living most of their lives online, decreasing the

---

87 Paul Dourish, *Where the Action Is: The Foundations of Embodied Interaction* (Cambridge, MA: MIT Press, 2001). See also Hiroshi Ishii & Brygg Ullmer, "Tangible Bits: Towards Seamless Interfaces Between People, Bits and Atoms" (1997) Proceedings of CHI97, ACM 234.

88 Dourish, *ibid* at 3.

89 Building on Dourish's model, tangible and embodied interaction now form a field of human-computer interaction research and design practice that focuses on the implications and new possibilities for interaction within the physical world. See for example, Hiroshi Ishii, "The Tangible User Interface and Its Evolution" (2008) 51:6 Comm ACM 32; Soraya Mostefaoui & Zakaria Maamar, eds, *Advances in Ubiquitous Computing: Future Paradigms and Directions* (Hershey, PA: IGI Global, 2008); Eva Hornecker & Jacob Buur, "Getting a Grip on Tangible Interaction: A Framework on Physical Space and Social Interaction" (2006) Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM 437; Elise van den Hoven et al, "Design Research and Tangible Interaction" (2007) Proceedings of the International Conference on Tangible and Embedded Interaction, ACM 109; Brygg Ullmer & Hiroshi Ishii, "Emerging Frameworks for Tangible User Interfaces" in John Carroll, ed, *Human Computer Interaction in the New Millenium* (NY: Addison-Wesley, 2001) 189; Mark Millard & Firat Soylu, "An Embodied Approach for Engaged Interaction in Ubiquitous Computing" in Julie Jacko, ed, *Human-Computer Interaction: Ambient, Ubiquitous and Intelligent Interaction* (Berlin: Springer, 2009) 464; Eva Hornecker et al, "TEI Goes On: Tangible and Embedded Interaction" (2008) 7:2 IEEE Pervasive Computing 91; Kenneth Fishkin, "A Taxonomy for and Analysis of Tangible Interfaces" (2004) 8:5 Journal of Personal and Ubiquitous Computing 347; Alissa Antle, Greg Corness & Milena Dromeva, "Human-Computer Intuition: Exploring the Cognitive Basis for Intuition in Embodied Interaction" (2009) 2:3 Intl J Arts and Technology 235; Dan O'Sullivan & Tom Igoe, *Physical Computing: Sensing, Controlling the Physical World with Computers* (Boston, MA: Thomson, 2004); and John McCarthy & Peter Wright, *Technology as Experience* (Cambridge, MA: MIT Press, 2004).

importance of physical space because we would transcend to a disembodied reality, and the bits running through servers would replace feet walking the streets. Weiser, however, envisioned a computing model that departed from the world of the conventional PC, as radical as the PC was from the world of the mainframe, computation that spread throughout the environment, and was embedded in the very fabric of the environment. This effectively and directly implicates our physical world, rather than replaces it, in the context of computing. In summary of the first salient feature of ubiquitous computing, physicality refers to computing being brought back into the real world, embedded in physical objects and physical environments everywhere. The physical nature of computing moving off the desktop and into our everyday lives encompasses the related and important aspects of mobility, augmented reality, hybridization and embodied interaction. Each of these aspects contributes to the paradigmatic shift in computing, one of computationally enhanced things, spaces and people, in which the power of computation is seamlessly integrated into all facets of our daily lives. Weiser's model of ubiquitous computing was also, paradoxically, one of invisible computers. The second salient feature of ubicomp, invisibility, is examined next.

2.2.2 Invisibility

Perhaps the most significant characteristic differentiating ubiquitous computing from the PC is its invisibility. Personal computers "cannot truly make computing an integral, invisible part of the way people live in their lives."[90] That is why it is imperative to "conceive a new way of thinking about computers in the world…that takes into account the natural human environment and allows computers themselves to vanish into the background."[91] Underlying Weiser's approach is the belief that invisibility in particular is a phenomenological human construct, an experience of being-in-the-world that is socially and psychologically created by humans as they go

---

[90] Weiser, "The World is Not a Desktop," *supra* note 18 at 7.

[91] *Ibid*.

about their various activities.[92] Weiser consistently held that he was drawing from and "inspired by" social scientists, philosophers and anthropologists to inform his vision of ubiquitous computing, although this appears to have been largely missed by many until recently.[93]

At its core, ubiquitous computing aims to be seamlessly woven into the fabric of the everyday world and the everyday life of people. For Weiser, "the most profound technologies are those that disappear." [94] Mahader Satyanarayanan interprets invisibility as a "complete disappearance of pervasive computing technology from a user's consciousness."[95] Kenneth Fishkin envisions "a progression towards a more real-world interaction style, where there is no perceived mediation, *i.e.*, an invisible user interface."[96] And for Donald Norman, "[t]he computer is really an infrastructure, even though today we treat it as the end object. Infrastructures should be invisible….A user-centered, human-centered humane technology where today's personal computer has not disappeared into invisibility."[97] Invisibility then can be said to consist of two concepts, invisibility in use and invisible infrastructures.

Weiser later reiterated the invisibility aspect of ubicomp by proposing childhood as the appropriate metaphor to reinforce the value of invisible technology: "playful, a building of foundations, constant learning, a bit mysterious and quickly

---

92 Heidegger, *supra* note 83; Weiser, "The Computer for the 21st Century" *supra* note 9 at 78.

93 A slide from Weiser's keynote talk at the Association for Computing Machinery (ACM) Symposium on User Interface, Systems and Technologies in 1994 titled "Building Invisible Interface?" reads "start from the arts and humanities; philosophy, phenomenology, anthropology, psychology, postmodernism, sociology of science, feminist criticism, your own experience" and followed by "this is the most important part of the talk. You may not get it on first hearing. Patience.", online: <http://www.ubiq.com/hypertext/weiser/UbiHome.html>. However, when Mark Weiser was diagnosed with cancer he decided to spend his remaining time writing a book on the real essence of ubiquitous computing to clear up some of the confusion around ubiquitous computing because, as told to PARC colleague John Seely-Brown, "they've completely missed the non-technical part of what ubiquitous computing is all about.": Department of Electrical Engineering and Computer Sciences, University of California Berkeley, "Mark Weiser dies at 46" (1999 obituary), online: UC Berkeley Electrical Engineering and Computer Sciences <http://www.cs.berkeley.edu/Weiser/bio.shtml>.

94 Weiser, "The Computer of the 21st Century," *supra* note 9 at 78.

95 Mahader Satyanarayanan, "Pervasive Computing: Visions and Challenges" (2001) 8:4 IEEE Personal Communications 15.

96 Kenneth Fishkin, "Embodied User Interfaces: Towards Invisible User Interfaces" (1998) Engineering for Human Computer Interaction 4.

97 Donald Norman, *The Invisible Computer* (Cambridge, MA: MIT Press, 1998) 13.

forgotten by adults. Our computers should be like our childhood, an invisible foundation that is quickly forgotten but always with us, and effortlessly used throughout our lives."[98] So, despite its omnipresence, supported by a dense communication network infrastructure, ubicomp is designed to get out of the way of what really matters, namely the activities that the technology is meant to be part of. Its invisibility emphasizes that the technology itself should be unnoticeable and recede into the environmental background that embeds human activities. Thus, it need not be necessarily, or literally, physically invisible.

Early investigations on the role of technology in society, as for example, McLuhan's study of media, demonstrated how pervasiveness can transform into invisibility.[99] All technologies that have matured and become socially acceptable seem to withdraw into the unnoticed, invisible background, like clocks and telephone cables. Weiser made these analogies, eyeglasses being one he highlighted, but he also compared computing to another revolutionary technology: writing.[100] This latter analogy made by Weiser is perhaps most prophetic because writing is everywhere and it no longer even seems like a technology or requires our attention the way a computer currently does. The embedded wireless nature of technologies means they will be too small to see or will be implemented in ways that are not noticeable even when we are looking for them. Taking Weiser's analogy of eyeglasses further, it is not just that the technologies are rarely noticed but easy to see, rather it is embedded in contact lenses.[101]

This notion of disappearance where a tool, as envisioned by Weiser, is literally visible, effectively invisible is drawn from philosophical principles. As he described,

---

98 Mark Weiser, "Creating the Invisible Interface" (1994) Proceedings of the 7th Annual Symposium on User Interface Software and Technology 1. Richard Gold makes similar analogies in his article "This is Not a Pipe" (1993) 36:7 Comm ACM 72.

99 In a 1964 essay, McLuhan states, "when a new media-induced environment becomes all-pervasive and transmogrifies our sensory balance, it also becomes invisible": Eric McLuhan and Frank Zingrone, eds, *Essential McLuhan* (New York: Basic Books, 1995) 226.

100 Weiser, "The Computer for the 21st Century", *supra* note 9 at 78.

101 Eyeglasses with laser and mirror devices are not capable of detection: Friedemann Mattern, "Wireless Future: Ubiquitous Computing" in *Proceedings of the Wireless Congress* (Munich, 2009), online: ETH Zurich, Distributed Systems Group <www.vs.inf.ethz.ch/publ/papers/mattern2004_electronica.pdf>.

"[a] good tool is an invisible tool. Invisible here meaning that the tool does not intrude on your consciousness; you focus on the task, not the tool."[102] The design of ubicomp applications is not primarily intended to interface directly with a human user, but rather designed more often to interact directly with the physical environment.[103] Given this design objective, ubiquitous technologies further withdraw into the background, just beneath our conscious recognition, because we will not necessarily deal with computers directly nor feel that we have much control over them.[104] In this way, from pencils to coffee pots, invisibility refers to the phenomena in which people directly employ tools without consciously being aware of them. Unlike cell phones, PDAs, laptops or ipads, ubicomp technologies, interfaces and networks are "invisible, everywhere computing that does not live on a personal device of any sort, but is in the woodwork everywhere."[105]

For Weiser and his PARC colleagues; "just as a good well-balanced hammer disappears in the hands of a carpenter and allows him or her to concentrate on the big picture, we hope that computers can participate in a similar disappearing magic act."[106] Embedded computers become "so unobtrusive we will not even notice our increased ability for informed action" where machines "take care of our unconscious details."[107] In other words, essentially invisibility in use, in which people directly employ tools without consciously monitoring them; working through them rather than working with them. Invisibility allows attention to be focused on the action rather than the

---

[102] Weiser, "The World is Not A Desktop" *supra* note 18 at 7.

[103] Anind Dey, Peter Ljungstrand & Albrecht Schmidt, "Distributed & Disappearing User Interfaces in Ubiquitous Computing" (2001) CHI 487; Kasmin Rehman, Frank Stajano & George Coulouris, "Interfacing with the Invisible Computer" (2002) CHI 213; Dourish, *supra* note 89, Chapter 1; Sarah Spiekerman & Frank Pallas, "Technology Paternalism: Wider Implications of Ubiquitous Computing" (2006) 4:1 Intl J Ethics of Science & Technology Assessment 1615.

[104] Dana Cuff, "Immanent Domain: Pervasive Computing and the Public Realm" (2002) J of Architectural Education 43.

[105] Weiser, "The World is Not a Desktop", *supra* note 18 at 8.

[106] Mark Weiser, Richard Gold & John Seely-Brown, "The Origins of Ubiquitous Computing Research at PARC in the Late 1980s" (1999) 38:4 IBM Systems Journal 693 at 695.

[107] Mark Weiser, "Open House" *ITP Review 2.0*; the web magazine of the Interactive Telecommunications Program of New York University (March 1996), online: Princeton University, Computer Science Department <http://www.cs.princeton.edu/courses/archive/spring99/cs598c/papers/wholehouse.doc>

connection. This is consistent with Weiser's human-centric model in which he emphasizes the psychological and social over the technical:

> [s]uch a disappearance of computers into the background is a fundamental consequence not of technology, but of human psychology. Whenever people learn something sufficiently well, they cease to be aware of it. When you look at a street sign, for example, you absorb its information without consciously performing the act of reading … when things disappear … we are freed to use them without thinking and so to focus beyond them on new goals.[108]

This invisibility or disappearance aspect of ubiquitous computing is essentially Martin Heidegger's analysis of the distinction between "ready-to-hand" and "present-to-hand," to describe the unconscious and conscious use of tools.[109] Borrowing from Heidegger, Weiser used the example of the way a skilled carpenter, engaged in his work, focuses on the use of the hammer and how it changes and is combined with other tools and materials, rather than focusing on the hammer itself. In other words, this process of accommodation and appropriation lets one focus on the use of the tool and not the tool itself, thus making the tool disappear. In a modern adaptation of the Heidegger 'hammer', when a computer mouse is used to complete some task, it becomes an extension of the body used largely unconsciously, but as soon as the mouse runs off the pad or the wire obstructs motion, or presumably if the wireless battery dies, it is 'present-to-hand' becoming consciously present as in use.[110]

The withdrawal or disappearance of the tool from the awareness of the user corresponds to its immersion into the background in the sense that the tool now becomes one more aspect of something taken for granted in our everyday lives. In this way, the seamless integration, or immersion, into the background referred to by Weiser means not only literally embedding the physical environment, but also embedding tools, or objects, in such a way that they do not interfere with the activities in which they are being used. As the technology becomes smaller and more powerful

---

[108] Weiser, "The Computer for the 21st Century", *supra* note 9 at 78.

[109] 'Ready-to-hand' refers to using things without thinking or analyzing them, but if for example, the object breaks, you start questioning its usefulness, hence the object is present-to-hand: Heidegger, *supra* note 85.

[110] Dourish, *Where the Action Is*, *supra* note 89 at 94.

with increased wireless connectivity "they allow computation to directly affect the real world without heavily instrumenting the environment."[111]

A second part to ubicomp's aim of computation receding into the background deals with infrastructure invisibility. As with using tools and invisibility, it means the physical, organizational and technological ability to become tacit in thought and action for users.[112] Electricity and plumbing systems are examples of infrastructure invisibility in the real world. Wires, voltage rules, power plants, pipes and sewage treatment centres are largely removed from our daily lives. Instead, we interact with these infrastructures through interfaces such as electrical outlets, light switches, faucets and toilets. These are the entry points through which we access the infrastructure. Flipping the light switch is a simple action, but underlying it is a vast and complex world. Electrical and plumbing infrastructures become visible when they break down, there are power outages or we have poor water pressure, bringing the processes and systems to the forefront of our consciousness.[113]

Similarly, wireless networks and electronic key cards are examples of current ubiquitous technologies with underlying infrastructures in place. Wireless networks require, for example; software drivers, installation of access points, management of access and passwords, all largely invisible to us. Electronic access cards have now commonly replaced keys and locks at least in the employment and business contexts, and involve the deployment of RFID readers, connection to a centralized access database, management of permissions and distribution of RFID embedded cards to authorized people, all of which entails the requisite technological, social and physical

---

[111] Roy Want, Trevor Pering, Gaetano Borriello & Keith Farkas, "Disappearing Hardware" (2002) 1:1 IEEE Pervasive Computing 36 at 42. See also Chris Noessel, Simona Pasque & Jason Tesler, "Interaction Design for Wireless" in Garfinkel & Rosenberg, *supra* note 26, Chapter 9; Pius Uzamere, Simson Garfinkel & Ricardo Garcia, "Bluejacked" in Garkinfel & Rosenberg, *supra* note 26, Chapter 20; Gordon Gow & Richard Smith, *Mobile & Wireless* (UK: Open University Press, 2006); Habib Ammari & Sajal Das, "Integrated Connectivity in Wireless Networks: A Two-dimensional Percolation Problem" (2008) 57:10 IEEE Transactions on Computers 1423; Katrina Michael and M.G. Michael, "Nanotechnology: The Growing Impact of Shrinking Computers" (2006) 1 IEEE Pervasive Computing 1.

[112] Norman, *The Invisible Computer*, *supra* note 99.

[113] *Ibid.*

infrastructure to allow the user to gain access with the simple action of swiping of the card, the actual interaction with the card and reader.

The challenge of making technology disappear, while at the same time having it always-on and always available to support everyday activities, points to an inherent tension within the ubicomp vision – a tension that Weiser identified when computational systems are invisible as well as extensive, because "it becomes hard to know what is controlling what, what is connected to what and what are the consequences."[114] To maintain "simplicity and control simultaneously" means finding a balance between "unlimited power and understandable straightforwardness."[115] This tension between disappearance and simplicity on the one hand and intelligibility and control on the hand means it may be impossible for people to recognize, let alone control, interaction with the ubicomp application. It also highlights the distinction between 'the disappearing computer' and the 'disappearing interface' or what Weiser called "calm technology."[116]

Technology should create calm. Let, for example, your shoes or pen communicate and work on your behalf rather than being subjected to the constant frustration, distraction and effort of the web, email, cell phones, and television. Despite the rather mundane contexts projected for ubiquitous computing, that of computers in everyday objects and places, by 1996 Weiser and Seely-Brown were predicting the coming age of calm technology:

> The most potentially interesting, challenging, and profound change implied by the ubiquitous computing era is a focus on calm. If computers are everywhere they better stay out of the way, and that means designing them so that people being shared by the computers remain serene and in control…[w]hen computers are all around, so that we want to compute while doing something else and have more time to be more fully human, we must radically rethink the goals, context and technology of the computer and all the other technology crowding into our lives. Calmness is a fundamental challenge for all technological design of the next fifty years.[117]

---

[114] Weiser, Gold and Seely-Brown, "The Origins of Ubiquitous Computing", *supra* note 19 at 694.

[115] *Ibid* at 695.

[116] Mark Weiser and John Seely-Brown, "Designing Calm Technology" (1996) 1 PowerGrid Journal 1, online: CiteSeerx <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.123.8091>.

[117] *Ibid* at 3.

Taking as their premise that human attention is a scarce resource, Weiser and Seely-Brown argue that we need to look at the design of technology that can be present in the everyday world without overwhelming us with demands for explicit attention. This seems to be a necessary condition if the aim is for a world where technology is dispersed throughout the environments we inhabit. Calming technology, therefore, is "that which informs but doesn't demand our attention."[118] Information technologies had already encroached enough on the quality of people's lives, an opinion shared by others who had already called for a reprieve from information overload.[119] However, the ubicomp vision, rather than call for less information, advocates that people should be provided with access to more information. The difference is the ability to have that information at the periphery and not at the centre of attention. Calm technology aims to reduce information overload by letting the user select what information is at the centre of their attention and what information is peripheral.

Weiser and Seely-Brown describe technology that moves between the periphery and the centre of our attention, outside of conscious awareness until we actively focus on it.[120] The result is "to put [it] at home, in a familiar place."[121] Technology that is so embedded, so pervasive, that it could be taken for granted. It would be informative without being overwhelming or distracting. Ubiquitous

---

[118] *Ibid*.

[119] See for example, Alvin Toffler, *Future Shock* (New York: Random House, 1970); Orrin Klapp, *Overload and Boredom: Essays in the Quality of Life in the Information Society* (New York, Greenwood Press, 1986); Guus Pijpers, *Information Overload: Managing Your Data* (Hoboken, NJ: Wiley & Sons, 2010); Harry Bruce, William Jones & Susan Dumais, "Information Behavior That Keeps Found Things Found" (2004) 10:1 Information Research, online: Information Research <http://informationr.net/ir/10-1/paper207.html>; Neil Postman, *Amusing Ourselves to Death* (New York: Penguin, 2006).

[120] Weiser & Seely-Brown, "Designing Calm Technology", *supra* note 118 at 4, used Natalie Jeremijenko's 'Dangling String' so-called artwork which she created while at PARC as an example of the periphery-centre behind calm technology; it is basically just what it says; an 8-foot piece of plastic string hanging down from a small electric motor mounted in the ceiling and connected via an Ethernet cable to the internet. The motor was programmed so that each bit of information flowing through the network causes it to perform a tiny twitch so when the network is quiet the string twitches a bit every few seconds, but when the network busy, the string whirls madly and emits the muffled, hollow noise of its own vibrations. It was installed at PARC intentionally in an unused corner where it could be seen and heard without being obtrusive. Weiser & Seely-Brown describe 'dangling string' as initially attracting attention but then fading into the periphery: "[a]t first, *Dangling String* creates a new centre of attention just by being unique, but this center soon becomes peripheral as the gentle waving of the string moves easily to the background." (at 4).

[121] *Ibid.*

computing would become "so commonplace, so unremarkable" that we should forget its enormous impact, just as we have with writing and electricity, two other ubiquitous technologies.[122]

One of the earliest and influential proponents of the post-PC, disappearing and calm computer movement is Donald Norman.[123] He takes the radio as a contemporary illustration of "where the technology of the computer disappears behind the scenes into task-specific devices that maintain all the power without the difficulties."[124] Norman describes the radio being perceived as a complicated device at first, but comes to be accepted as it is built and concealed in other objects or furniture. He goes on to develop scenarios for an intelligent, reactive and serving environment, not unlike Nicholas Negroponte's "intelligent agents," a kind of digital butler that does all your work for you while you take it easy.[125] Norman's intent is to alleviate the complexity and frustration of what he perceives exists with current technology.

Weiser's scenario of Sal, a Silicon Valley executive and mother, describes a day in her life to illustrate calm computing.[126] As Sal moves from her domestic world to her work place she is perpetually informed of what is going on with her family, neighbours, fellow citizens and work colleagues. As a result, Sal is able to keep up-to-date, avoid obstacles, make the most of her time and conduct work, all smoothly and effortlessly. It begins,

---

[122] *Ibid* at 2.

[123] Computing invisibility/calmness began with Weiser, but became popularized by Donald Norman, *The Invisible Computer*, *supra* note 99.

[124] *Ibid* at viii.

[125] Nicholas Negroponte, *Being Digital* (NY: Random House, 1995) 150-151. See also William Buxton "Less is More (More or Less)" in Paul Denning, ed, *The Invisible Future: The Seamless Integration of Technology in Everyday Life* (NY: McGraw-Hill, 2001) 145; Buxton describes himself as a "skeptomist, half skeptic and half optimist" because he is discouraged by what he has seen over past 30 years of technology not meeting social and human benefits yet marvels at technological advances that have been made.

Note also, Weiser recounts a story of when he and Negroponte were on stage together at the MIT Media Lab engaged in an argument in front of some 700 people during which Negroponte was, according to Weiser, "rhapsodizing" about a world filled with computerized "intelligent agents" who will answer all our needs and Weiser taking the position that a butler would be fun but ultimately "distracting and intrusive." The defining words for Weiser "will not be 'intelligent' or 'agent' but rather 'invisible' and 'calm and 'connection.'" Weiser, "Open House", *supra* note 109.

[126] Weiser, "The Computer for the 21st Century", *supra* note 9 at 89.

> Sal awakens: she smells coffee. A few minutes ago her alarm clock, alerted by her restless rolling before waking, had quietly asked: 'coffee?' and she mumbled 'yes'…Sal looks out her windows at her neighbourhood. Sunlight and a fence are visible through one, but through others she sees electronic trails that have been kept for her of neighbours' coming and going during the early morning. Privacy conventions and practical data rates prevent displaying video footage, but time markers and electronic tracks on the neighbourhood map let Sal feel cozy in her street.[127]

This short excerpt depicts a world that revolves around Sal's assumed preferences, where computers, cameras and sensors are embedded into her world to make her life efficient, smooth and calm. Sal seemingly glides through a life where everything is done or laid out for her and whenever there is potential for frustration, such as a traffic jam or parking problem, the invisible computers come to her rescue and gently inform her of what to do and where to go. A motivation behind ubicomp therefore is to make our lives convenient, comfortable and calm, but also informed. This means there is the necessity of having some sort of awareness of context. Invisible and calm computing is possible when a system of inter-connected devices is 'aware' of the task or activity of the user and cohesively adjusts the system based on this awareness to help facilitate the user's activity.[128]

To summarize this section on 'invisibility,' the ubiquitous computing paradigm envisions technology becoming invisible in people's everyday lives; in which the computing elements and their inter-communication are largely hidden from the user. The technology is not readily visible, it is worn or embedded in building infrastructure and is spoken with and related to. Weiser believed computing ought to disappear into the fabric of our lives so users are freed from the burden of the PC. Central to this belief was that computing use has to be so easy that it no longer requires thinking or the

---

127 *Ibid*.

128 *Ibid*. In the last abstract of a paper Weiser would never publish due to his untimely death, he intended to describe in greater detail the interplay and dependencies between invisibly calming technology and the pervasive connectivity infrastructure, key functions to the realization and effectiveness of the original vision of ubicomp. The abstract for a paper tentatively called "Calm Technology & Pervasive Computing" he wrote, "[i]n the 21st century the technology revolution will move into the everyday, the small and the invisible. The impact will increase ten-fold as it is embedded in the fabric of everyday life. As technology becomes more embedded and invisible, it calms our lives by removing the annoyances while keeping us connected with what is truly important. This embedding, this invisibility, this radical ease-of-use requires radical innovations in our connectivity infrastructure." Roy Want, "Remembering Mark Weiser: Chief Technologist, Xerox PARC" (2000) 7:1 IEEE Personal Communications 8, 8.

computer has to be intelligent enough that it no longer requires explicit user input. That way it can fade into the background. To achieve this, computers must be 'aware' to adapt to behaviour and context. By "vanishing computers into the background…computers will become invisible to common awareness" and people will simply use them unconsciously to accomplish everyday tasks."[129] In other words, computing which is context-aware; the third salient feature of ubiquitous computing.

2.2.3. Context-Awareness

Ubiquitous computing derives from the information era and the idea that we can freely plug in more information providers and consumers into a public infrastructure with devices that are always-on, wirelessly connected and mobile. Context-awareness adds another dimension by converting the reams of raw data into information and knowledge, with the idea of getting the right information to the right person at the right time. The convergence of these two ideas results in the computational devices embedded in physical and social situations achieving a better understanding of, and interaction with, the physical environment.[130] Although Weiser did not define his approach as 'context-aware' it is relatively easy to see the roots for it implanted in his vision.[131] In order for computers to fulfill Weiser's vision, they must be able to sense their surroundings and they need to communicate with other computational objects. It is this computational reach that makes 'everywhere,' 'seamless' and 'invisible' computing possible.

Context-aware computing endeavours to enhance computing technology with the capability to sense, and reason about, human context.[132] In effect, context-aware

---

[129] *Ibid* at 98.

[130] Thomas Moran & Paul Dourish, "Introduction to this Special Issue on Context-Aware Computing" (2001) 16:2-3 Human Computer Interaction 87

[131] The term 'context-aware' was formally introduced by Bill Schilit & Marvin Theimer, "Disseminating Active Map Information to Mobile Hosts" (1994) 8:5 IEEE Network 22. See also Bill Schilit, Norman Adams & Roy Want, "Context-Aware Computing Applications" in *Workshop on Mobile Computing Systems and Applications* (Santa Cruz, CA: IEEE, 1994) 85.

[132] Anind Dey, "Understanding and Using Context" (2001) 5:1 Personal Ubiquitous Computing 4-7; James Crowley et al, "Perceptual Components for Context Aware Computing" (2002) 2498 Ubicomp 2002: Ubiquitous Computing, Lecture Notes in Computer Science 117-134; A Fuji, "Trends and Issues in Research on Context Awareness Technologies for a Ubiquitous Network Society" (November 2008) NISTP Science

computing compensates for limitations in human cognition through the use of sensor-based and computational tools. It seeks to overcome and extend human attention, memory, comprehension and decision making. By examining and reacting to a user's context to help promote and mediate people's interactions with each other, and their environment, context-awareness focuses on detecting, identifying and locating people's movements, routines and actions. But, what is context?

Although there appears to be no consensus on the meaning of both context and context-aware computing, what constitutes context is generally viewed, within the computer science and HCI research community, as something that can be continuously sensed and measured using location, time, person and activity type dimensions. Pioneers of context-aware computing, Bill Schilit and Marvin Theimer, define context as location, identities of nearby people, objects and changes to those objects, largely reflecting Weiser's notion of location in terms of measurable spatial information as the main contextual premise.[133] They consider where you are, whom you are with and what resources are nearby to be the important aspects of context. Others have since recognized that there is more to context than position, encompassing not just where, who and what but also when and why. Within this expanded framework, Anind Dey and Gregory Abowd define context as "any information that can be used to characterize the situation of an entity. An entity is a person, place or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves."[134] This means that any information that depicts the situation of a user can be entitled context. Diego Lopez de Ipina, et al, go somewhat farther in delineating the common attributes of context to include identity, location, time,

---

and Technology Trends 092; Carly Weeks, "The Smart Phone That Knows What you Are Thinking" *The Globe and Mail* (January 2012), online: The Globe and Mail <http://www.theglobeandmail.com/technology/the-smart-phone-that-knows-what-you-want/article542362/>.

[133] Schilit & Theimer, *supra* note 133 at 1.

[134] Anind Dey & Gregory Abowd, "Towards a Better Understanding of Context and Context-Awareness" (2001) GVU Technical Report GIT-GVU 99-22, online: Georgia Tech Library SMARTech <http://smartech.gatech.edu/handle/1853/3389> at 3. See also Albrecht Schmidt et al, "There is More to Context than Location" (1999) 23 Computers & Graphics 893.

elements of the natural environment, physiology, activity and social interaction.[135] Similarly, Philip Agre describes context as physical or architectural, practices or routines for doing particular things in a particular place, and institutional or social roles and rules.[136] Ubicomp then, through the use of enabling technologies, makes it possible for inferences to be made from all of these defining contextual aspects.

It is critically important, however, to take from these definitions not just the informational aspect of context awareness, but also that context refers to the physical and social situation in which computational devices are embedded. The physical environment in which human activity is experienced is especially important because ubiquitous computing occurs in the context of everyday life. Or conversely, context plays a central role in ubiquitous computing because computation moves off the desktop into the physical world and context-aware systems mediate between people and real-world places.[137]

Just as there is more to context-awareness than location, 'place' means more than just location.[138] Geographic location and material form relate to physicality, whereas the humanistic meaning of place refers to the types of behaviour that may be expected in particular places. Certain values[139] and meanings are invested into particular places. For example, different behaviours are expected in a bar than in a church. Moreover, people may behave differently in different places, even when engaged in the same activity. For example, eating at home or eating at a restaurant. Therefore, in addition to the informational context, or the 'what' and 'when', there are two additional key aspects of context that are equally important; the spatial context –

---

[135] Diego Lopez de Ipina et al, "TRIP: A Low Cost Vision-Based Location System for Ubiquitous Computing" (2002) 6:3 Personal and Ubiquitous Computing 206; George Tsibidis, Theodoros Arvanitis & Chris Baber, "The What, Who, Where, When, Why and How of Context-Awareness" (Paper delivered at the Human Computer Interaction Conference, The Hague, Netherlands, April 2000), online: Georgia Tech Library SMARTech <http://smartech.gatech.edu/jspui/bitstream/1853/3464/23/00-18x.pdf>.

[136] Philip Agre, "Changing Places: Contexts of Awareness in Computing" (2001) 16 Human-Computer Interaction 177.

[137] Victoria Bellotti & Keith Edwards, "Intelligibility and Accountability: Human Considerations in Context-Aware Systems" (2001) 16:2-4 Human-Computer Interaction 193 at 199.

[138] An examination of the concept of 'place' is covered in Chapter Four.

[139] Helen Nissenbaum et al, "Privacy and Contextual Integrity: Framework and Applications" (May 2006) *Proceedings of the 27th IEEE Symposium on Security & Privacy* 184.

where you are, and the social context – who you are with. From these factors, the 'why' can be determined or surmised. Therefore, the combined effect of context-aware technologies means that the network can detect and respond to the environment, or context, often without human intervention, thus creating electronic environments that are sensitive and responsive to the presence of people and things, hence the emergence of a 'smart world.'

Ambient Intelligence (AmI)

In the 1950s, a few years after the computer was born, Alan Turing planted the seed for intelligent computing by raising the question, "Can machines think?"[140] He predicted by the end of the century "the use of words and general educated opinion will have altered so much that one will be able to speak of machines thinking without expecting to be contradicted."[141] The question, actually, became "can things think?" then "when things start to think" before the end of the century.[142] Thing thinking means the thing has some intelligence.[143] Today, the question that might be asked is 'can intelligent things be everywhere?'

Ambient intelligence, or AmI, is a pervasive and unobtrusive intelligence in the surrounding environment, supporting the activities and interactions of the users.[144] It refers to a world of computing technologies in which people are empowered through a digital environment that is aware of their presence and context, and is sensitive, adaptive and responsive to their preferences, needs, habits, gestures, actions and

---

[140] Alan Turing, "Computing Machinery and Intelligence" (1950) 59 Mind 433 at 433.

[141] *Ibid*.

[142] Neil Gershenfeld, *When Things Start to Think* (New York: Henry Holt & Co, 1999).

[143] "Things That Think Consortium", online: MIT Media Lab <http://ttt.media.mit.edu/>.

[144] Giuseppe Riva et al, "Presence 2010: The Emergence of Ambient Intelligence" in *Being There: Concepts, Effects and Measurement of User Presence in Synthetic Environments* (Amsterdam: IOS Press, 2003); Pasi Ahonen et al, "From Ubiquitous Computing to Ambient Intelligence" in David Wright et al, eds, *Safeguards in a World of Ambient Intelligence* (Berlin: Springer, 2008) 1; Donald Norman, *The Design of Everyday Things* (New York: Basic Books, 2002); Tom Igoe & Dan O'Sullivan, *Physical Computing: Sensing and Controlling the Physical World with Computers* (Boston: Thomson Course Technology, 2004); Emile Aarts & José Encarnação, eds, *True Visions: The Emergence of Ambient Intelligence* (Berlin: Springer, 2006); Yang Cai & Julio Abascal, eds, *Ambient Intelligence in Everyday Life* (Berlin: Springer, 2006); Juan Carlos Augusto & Daniel Shapiro, *Advances in Ambient Intelligence* (Amsterdam: IOS Press, 2007); and José Encarnação, "Ambient Intelligence: The New Paradigm for Computer Science and for Information Technology" (2008) 50:1 IT Information Technology 5; and Adam Greenfield, *Everyware, supra* note 11.

emotions. All of the physical and digital environment around us – homes, offices, cars and cities – will collectively develop into a pervasive network of intelligent devices that will cooperatively gather, process and transport information. Therefore, AmI is an extension of ubiquitous computing; people surrounded by simple interfaces that are embedded in all kinds of objects and by an everyday environment that is capable of recognizing and responding to individuals in a seamless, unobtrusive and invisible way. The promise of ambient intelligence fulfills Weiser's vision of removing computation to the background where technology adjusts to suit humans instead of us adjusting to technology.

There are basically five layers of ambient intelligence, all of which build on Weiser's ubicomp vision. First, ambient intelligence is embedded in the environment. Many networked devices are integrated into the environment, both in the physical sense – hidden in walls, clothing and packaging – and in the social sense, as it is possible to communicate with it in a 'natural' way, for example by movement or speech.[145] Second is the context-aware layer in which devices can recognize you and your situational context. Technology responds to what happens around it by detecting movement, reading RFID chips, or recognizing speech. Third, personalization; devices can be tailored to your preferences and needs. In other words, the capacity to adjust, which means ambient intelligent computing not only detects its environment, but adjusts to it in a personalized manner. Personalization in the AmI system can retrieve a person's profile and set up interaction with technology that is tailor-made to suit the person. Fourth, the adaptive layer, which means systems and technologies that can change in response to you. And fifth, anticipation; your preferences and needs are anticipated without conscious direction. Hence, computing that is not only embedded and responsive, but can also think ahead. The car, for example, something Weiser was particularly excited about because he did not want to be bothered with "operating" the

[145] Emile Aarts & Stefano Marzano, *The New Everyday: View of Ambient Intelligence* (Rotterdam: 010 Publishers, 2003); Peter J Denning, ed, *The Invisible Future: The Seamless Integration of Technology into Everyday Life* (New York: McGraw-Hill, 2002).

complex systems involved in car driving.[146] The 'smart' car anticipates the movements of other drivers and adapts its speed automatically if other drivers suddenly brake, accelerate or switch lanes.

Smart homes, smart appliances, smart cars, smart highways, smart airplanes, smart shoes and smart offices all arise from pervasive, unobtrusive computational intelligence in the surrounding environment supporting the activities and interactions of the users. For example, instead of reaching for the remote to change the television channel, a smart entertainment system will do it for us. In the field of elderly care, detectors can sound the alarm if someone falls out of bed or tries to leave the house at an unusual time. The walls can, literally, grow ears, by responding to certain sounds in rooms, such as a cry for help or a desperate question as to where someone has left her keys. Toilets can test urine automatically in order to spot health problems quickly. And there are countless other applications conceivable, including for example, by inserting an RFID chip into a refrigerator, it can recognize the food inside to help you write your shopping lists, or it can shop for you, or give feedback on eating habits and make suggestions for menus. Retailers can automate the payment and stock system extensively if all products are equipped with chips that can be read automatically by the checkout. A mobile phone with GPS aids parents in tracking down their children if they are lost. Devices, or objects, in houses can respond to the presence or even the moods of people in them by, for instance, adjusting the intensity of the lighting, allowing incoming telephone calls to come through or not, by making coffee when someone wakes up, or monitoring your children's safe arrival home from afar.

The on-going development of intelligent systems and initiatives reflect a combination of political, economic and cultural factors motivating the production, use and convergence of new technologies to locate, track and monitor people and things.[147] These factors include a shift towards a safety and security state, a desire to realize the potential profitability of integrated and accelerated forms of organizational

---

[146] Weiser, "Creating the Invisible Interface", *supra* note 100.

[147] Colin Bennett & Lori Crowe, "Location-Based Services and the Surveillance of Mobility: An Analysis of Privacy Risks in Canada" *Report to the Office of the Privacy Commissioner of Canada* (June 2005) 8.

management and a cultural commitment to efficiency, productivity, convenience and comfort.[148] Clearly, there are compelling advantages to accurate, continuous, real world, real time enhancement capabilities. Emergency services are better able to find accident victims. Commercial organizations can improve the way they do business by fleet, product and employee tracking. Retailers, stadiums and other service oriented facilities can adjust staffing levels and inventory to best accommodate demand and patterns. Caregivers can secure location devices on or in the bodies of children or the elderly. Government intelligence, law enforcement, port and custom authorities, as well as correctional facilities, can manage risk with increased security applications for the purpose of locating and monitoring. The health care industry can improve services and delivery through a host of applications, from electronic records to mobile accessibility and care. Yet, for all of the benefits and advantages, there is a catch. There are implicit privacy and data protection risks when physically embedded technologies facilitate the capture and sharing of more of our personal and spatial contexts.[149]

To conclude this section on the third salient feature of ubiquitous computing, context and context-awareness provides computing environments with the ability to usefully adapt the services or information they provide. It is the ability to implicitly sense and automatically derive the user needs that separate physically embedded context-aware applications from traditionally focused data processing applications. This design shift adds intelligent functions and facilitating systems which are more attentive, responsive and aware of the user's identity and the user's environment. Ambient intelligent systems are inherently context-aware because they react, adapt and anticipate actions and events. This represents the ultimate realization of Weiser's vision of ubiquitous computing by seamlessly integrating computing devices into the physical world which work in concert to support people in carrying out their everyday life activities in a simple, natural way using information and intelligence hidden in the network connecting these devices.

---

[148] *Ibid*.

[149] The surveillance and privacy implications arising from the ubiquitous computing paradigm are addressed in Chapter Two.

2.3 Ubiquitous Computing: Are We There Yet?

Like other computing paradigms before it, this vision guides the direction of technical developments as much as it predicts them.[150] The ubiquitous computing vision is still about intuitive, unobtrusive and distraction-free interaction with omnipresent, technology-rich environments. To bring interaction 'back to the real world' after an era of keyboard and screen interaction, the evolution of ubiquitous computing has undergone what has been described as three generations of research and development; connectedness, awareness and smartness.[151] The first generation aimed towards autonomic systems and their adaptation was driven by the availability of technology to connect literally everything to everything. Networks of ubiquitous information and communication systems emerged, "forming communication clouds of miniaturized, cheap, fast, powerful, wireless connected, and 'always on' systems, enabled by the massive availability of miniaturized computing, storage, communication, and embedded-systems components."[152] The second generation added sensor based recognition systems as well as knowledge processing and representation. The result was systems that capture, recognize, organize and manage context and knowledge with respect to the environment autonomously. Building on connectedness and awareness, a third generation attempts to exploit the semantics of ubiquitous computing systems, services and interactions. In other words, it seeks to give meaning to situations and actions, or behaviours and intelligence to systems.

Therefore, has Mark Weiser's vision of ubiquitous computing been realized? Computing has for many of us become an integral part of our world, in which gadgetry, off the desktop, is used without thinking much about it. Some technologies have become invisible and others embedded in devices we use. Mobile cell phones are currently the prime computing platform and tablet computers are a fast growing market. Televisions are now computers enhanced with hard drives, networking capabilities and special user interfaces. Most cars now routinely have a GPS, or the

---

[150] Bell & Dourish, "Yesterday's Tomorrows", *supra* note 15.

[151] Alois Ferscha, "20 Years Past Weiser: What's Next?" (2012) 11:1 IEEE Pervasive Computing 52-61.

[152] *Ibid* at 53.

option for installing a GPS. As the cost of display technologies shrinks, digital displays are replacing traditional billboards, posters and signs. More and more, the digital permeates the physical space in a seamless manner. Wireless and mobile communication technologies are already widely deployed and their capabilities are increasing. Domestic, commercial and public infrastructures are being enhanced with computation providing enhanced assistance and services. The home, for example, is being transformed with automated operations such as lighting, temperature, entertainment systems, kitchen facilities, space monitoring and smart appliances such as networked and wirelessly controlled washing machines and refrigerators. Commercial practices are redefined through wireless networking, RFID tagging and remote monitoring, thus increasing supply chain efficiency and adding customer value. Public places are augmented with sensors placed - for example, in airports, hospitals, museums, universities, amusement parks, stadiums and transit systems – to aid activities related to work, education, entertainment, healthcare and law enforcement. The desktop computer has not been displaced, but augmented. And Weiser was entirely correct that the purposes to which people would put computational devices are not radically new ones, but rather reflect existing social and practical needs as well as supporting everyday activities. Although we are not completely there yet, significant steps towards Weiser's vision of ubiquitous computing have already arrived.

Its arrival into the physical everyday world began, roughly, in 2005, when Apple put out the first iPod shuffle, Adidas launched the adidas1 shoe and iRobot introduced the Roomba Discovery vacuum cleaner, none of which looked like a traditional computer. Also, by 2005, a range of industry factors made possible the efficient development of products that fit Weiser's vision of ubiquitous computing as software, hardware and networks no longer had to be integrated from scratch as they had been throughout the 1990s.[153] Moreover, the explosion of the RFID market at this time is

[153] Mike Kuniavsky, *Smart Things: Ubiquitous Computing User Design Experience* (Burlington, MA: Elsevier, 2010)10.

seen by many as marking the dawn of ubiquitous computing.[154] It continued to gain momentum from technological progress in electronics miniaturization, network connectivity with new wireless communication standards, and the exponentially growing Internet, that is, the evolution of technologies that can literally connect everything to everything. Building on networks and connectivity, sensor-based recognition systems have emerged which add context-awareness and intelligence to computation.[155]

Ubiquitous computing has traditionally been positioned in the future, a potential state that may or may not be fully reached.[156] Assuming ubicomp is always in the future significantly underestimates the deep intertwining that has already happened between embedded technology and everyday life. Indeed, "if the availability of devices with wireless communications and powerful computational properties is anything to go by, then it is hard to deny that computation is already ubiquitous."[157] We already live in a ubiquitous computing world that is growing more so by the day. Projections claim that the number of currently active mobile phones in the world will exceed the number of people within the decade.[158] If this comes to pass there will be more than one mobile phone, more than one network connected computer, more than one ubiquitous computing device, per person. Everywhere.

3. Conclusion

Over two decades ago, Xerox PARC researcher Mark Weiser coined the term and defined the field of ubiquitous computing in his seminal work, "The Computer for the

---

[154] ITU Telecommunication Standardization Sector, *ITU-T Workshop Report on Networked RFID: Systems and Services, Geneva, 2006* (Geneva, ITU-T, 2006), online: International Telecommunication Union <http://www.itu.int/ITU-T/worksem/rfid/>; Greenfield, *Everyware*, *supra* note **Error! Bookmark not defined.**; see also RFID World, <http://www.rfidworld.ca>.

[155] Albrecht Schmidt et al, "Interacting with 21st Century Computers" (2012) 11:1 IEEE Pervasive Computing 22.

[156] Bell & Dourish, "Yesterday's Tomorrows", *supra* note 15.

[157] *Ibid* at 142.

[158] "Finishing the Job" *The Economist*, A Special Report on Telecoms in Emerging Markets (26 September 2009) 13, online: The Economist <http://www.economist.com/node/14483856>.

21st century." After Vannevar Bush's "As We May Think" set the tone for "a new relationship between thinking man and the sum of our knowledge,"[159] Weiser's ideas shifted the focus from Bush's virtual world towards the relationship between our lives and the sum of our technology[160]. While such ideas likely seemed utopian at the time, progress in computing and connectivity together with the sophistication and availability of enabling technologies is evidence that Mark Weiser's vision is being executed. This represents a huge paradigmatic shift in computing which impacts our daily life, certainly, and potentially our social values and core beliefs. With its large applicability across public and private, personal, business and public sector domains, developments in ubiquitous computing affect all of our lives, all of the time.

As the field of ubiquitous computing matures, more of the key issues start shifting away from the technical challenges to those that have a fundamentally social orientation. How are we to use those smart devices in our daily routine? When should they be turned on and off? Who and what should they be allowed to see, feel, or hear? Among such questions, privacy is a primary concern when it comes to assessing the effects of a widespread deployment of ubiquitous computing.

Chapter One examined the emerging technological landscape of ubiquitous computing. Three of its key characteristics, physicality, invisibility and context-awareness, reinforce the guiding principle of making computers vanish into the background. Yet, by virtue of these very definitions and characteristics, ubiquitous computing creates new and unique privacy concerns. Among these concerns are the enhanced surveillance capabilities. The surveillance of daily lives, made possible through the implementation and of ubiquitous and ambient technological systems and apparatuses, is permeating the spaces of the everyday.

Many of the larger questions about control over informational privacy and data protection have already been asked of other technologies. Yet, when other people can take control over one's information, they potentially take away one's control over their

---

[159] Vannevar Bush, "As We May Think" *Atlantic Monthly* (July 1945) 101, online: The Atlantic <http://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/303881/>.

[160] Wayt Gibbs, "As We May Live" (November 2000) Scientific American 36.

private space. The spatial interests which privacy seeks to protect are more directly and more pervasively compromised by the seamless integration of ubicomp technologies into the spaces and places of our everyday lives. The 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. 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 there are both information and spatial dimensions to privacy, "linking privacy to informational transparency tends to mask a conceptually distinct privacy harm that is spatial."[161] Without an assessment that more broadly considers people and their spaces, we risk these interests being collapsed into the informational paradigm, further marginalizing core interests that individuals have in sustaining physical and personal space. This is rendered more pressing because ubiquitous computing technologies are creeping into our physical world largely unnoticed. Chapter Two explores the surveillance issues and discusses the emerging privacy implications, re-asserting the importance of spatial privacy as computing technology comes back into the real world.

[161] Julie Cohen, "Privacy, Visibility, Transparency and Exposure," (2008) 1 *University of Chicago Law Review* 75.

CHAPTER TWO

SURVEILLANCE AND PRIVACY IMPLICATIONS OF UBIQUITOUS COMPUTING

> *In engaging with a technology so entirely friendly toward surveillance, spying, privacy invasion and ruthless technical intrusion on previously unsoiled spaces, we are playing with fire. Nothing new here – fire is two million years old. It helps to learn about fire and its remarkable affordances. Not a lot is to be gained by simply flinging lit matches.*
>
> Bruce Sterling, *Shaping Things* (2005)

1. Introduction

The original vision of ubiquitous computing emphasized that computing needed to leave the desktop and move out into the spaces and places of everyday life through a network of 'smart' objects. This paradigm was very different from how people imagined 'computers' in the 1990's. At a time when connecting to the Internet required a desktop interfaced via a screen, a keyboard, and a mouse, the idea of networked interactions via 'computers' spread across working, home and public environments in the form of sensors, context-aware technologies, RFID tags and mobile devices seemed unlikely, even scary.[1] Although privacy was not originally part of the ubicomp agenda, it became an "unexpected problem" in response to newspaper headlines about "big brother coming to the office."[2] One of PARC's first prototypes, the Active Badge,[3] was

---

[1] Mahadev Satyanarayanan, "Pervasive computing: Vision and Challenge" (2001) 8:4 IEEE Personal Communications 10–17.

[2] Mark Weiser, Rich Gold & John Seely-Brown "The Origins of Ubiquitous Computing Research at PARC in the late 1980's" (1999) 38:4 IBM Systems Journal 693 at 694.

[3] The "Active Badge" was a small, wearable device that transmitted a unique infrared signal every ten seconds to a network sensor, which could then accurately identify the transmissions and pinpoint the device's location. Initially conceived and deployed to help the receptionist at the PARC Lab more accurately

not intended to spy on anyone, but as Adam Greenfield describes, "it was readily apparent how the system could be abused, especially when the device responsible was so humble and so easy to forget about. Original sin came early to ubicomp."[4] Today's 'active badge' might be characterized as the 'embedded badge', essentially performing the same functions as the active badge, but now developed and refined with enhanced tracking capabilities extending well beyond the receptionist's desk into our everyday lives. Even at the most basic level, "it would be difficult to imagine a technology more suited to monitoring a population than one sutured together from RFID, GPS, networked biometric and other sensors, and relational databases. Everyware [*sic*] redefines not merely computing but surveillance as well."[5]

---

forward telephone calls from the front desk to the call's recipient, but was also used as an indoor tracking system: Roy Want et al, "The Active Badge Location System" (1992) 10:1 ACM Transactions on Information Systems 91; Mark Weiser, Rich Gold & John Seely-Brown, "Origins of Ubiquitous Computing" (1999) 38:4 IBM Systems Journal 693. For the receptionist, the system was a "boon" (at 97), but for those being tracked, there were more complicated reactions, including social fears, and concerns about violations of personal freedom and individual privacy rights (at 99-101). The Active Badge was always intended as an extension of other forms of office systems and management, like phone systems, fire alarms, security and climate control. Yet between 1989 and 1992, as the system was deployed in universities, research centres, labs and workplaces, debates escalated about the merits of tracking, mechanisms for thwarting the system and the politics of surveillance: Robert Harper et al, "Locating Systems at Work: Implications for the Development of Active Badge Applications" (1992) 4:3 *Interacting with Computers* 343; Robert Harper, "Looking at Ourselves: An Examination of the Social Organizations of Two Research Laboratories" in *Proceedings of the ACM Conference on Computer-Supported Cooperative Work* (New York: Association for Computing Machinery, 1992) 330; Philip Agre, "Conceptions of the User in Computer System Design" in Peter J Thomas, ed, *The Social and Interactional Dimensions of Human-Computer Interfaces* (Cambridge: Cambridge University Press, 1995) 67.

[4] Adam Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing* (New York: New Riders, 2006) 19.

These types of references to surveillance as sin tend to invoke dystopic privacy fears. Most commonly, the expression of these fears adopt the implicit metaphor of Big Brother, a metaphor that has so strongly shaped understandings of privacy that Daniel Solove argues that even when people do not explicitly mention Big Brother or Orwell, they still draw from a privacy framework conceptualized through the metaphor of Orwell's famous novel *1984*. However, while the metaphor of Big Brother has shaped legal thought, Solove, like others, argues that it is no longer analytically useful because the all-seeing surveillance structure imagined inside that framework has been replaced (if it ever existed) by new forms of surveillance: "Privacy and Power: Computer Databases and Metaphors for Information Privacy" (2001) 53 Stanford Law Rev. 1393-1462. For Matt Adams, "we are still locked in an Orwellian paradigm that has long since passed its sell by date." Quoted in Adriana de Souza e Silva & Daniel Sutko, "An Interview With Matt Adams from Blast Theory" in A de Souza e Silva & D Sutko, eds, *Digital Cityscapes* (New York: Peter Lang, 2009) 71-83, 81. Notwithstanding, warnings of Orwellian state scrutiny remain commonplace.

[5] Greenfield, *Ibid* at 108.

Yet, public compliance and acceptance of surveillance in many aspects of modern life largely continues without protest.[6] This dichotomy between human instinct and everyday reality has been explained as surveillance actually having two faces.[7] The stimulus for the proliferation of surveillance in our everyday lives is not the need for social control, but rather the changes in the order of society.[8] Surveillance is often a necessity due to the way we structure our political and economic relationships in a society that values mobility, speed, security, and consumer freedom.[9] The same systems, therefore, that may be feared for their power to watch and keep track of our personal lives are established, and acquiesced to[10] in order to protect and enhance our lives.[11] We are, then, "of two minds about surveillance. On the one hand it is creepy, Orwellian and corrosive of civil liberties. On the other hand, it keeps us and our

---

6 Hille Koskela, "CamEra: The Contemporary Urban Panopticon" (2003) 1:3 Surveillance & Society 292-313. Koskela further notes that this compliance and acceptance of surveillance technologies has afforded the introduction of unparallelled levels of both overt and intimate modes of monitoring, increasingly specialized and prevalent within both public and private domains. See also Mark Poster, "The Information Empire" (2004) 4:3 Comparative Literature Studies 317-334 (coined the term 'participatory surveillance' to describe the ways in which users of new technologies are complicit in the loss of privacy). See also William Staples, *The Culture of Surveillance: Discipline and Social Control in the United States*, (New York: St. Martin's Press, 1997) discussing the normalization of surveillance and the public's acceptance of being watched most of the time in exchange for convenience and safety. Similarly, Luann Lasalle stated in the Globe and Mail, describing location-aware technologies, "[t]hese are great services if you're knowledgeable of the tradeoff, if you understand what you're giving up to get the service": "Where Google meets Facebook meets GPS" (29 February 2009) *The Globe and Mail*, p. L3, <http://www.theglobeandmail.com/life/article10137.ece>; and for Mark Monmonier, what was remarkable about the growth of aerial mapping was that, despite its potentially intrusive nature, few concerns were raised. Until "one's whereabouts was so easily determined, archived, and sold, locational nakedness was hardly an issue.": *Spying With Maps: Surveillance Technologies and the Future of Privacy* (Chicago: University of Chicago Press, 2002) 175.

7 David Lyon, *Surveillance Society: Monitoring Everyday Life* (Buckingham, UK: Open University Press, 2001) at 3.

8 *Ibid*.

9 *Ibid*.

10 Some would say begrudgingly at best. See for example, John Gilliom, "Struggling with Surveillance: Resistance, Consciousness and Identity" in Kevin Haggerty & Richard Ericson, *The Politics of Surveillance and Visibility* (Toronto, ON: University of Toronto Press, 2006) 111.

11 David Lyon, "Surveillance Studies: Understanding Visibility, Mobility and the Phenetic Fix" (2002) 1:1 Surveillance & Society 1-7, 4; Graham Sewell & James Barker, "Neither Good, nor Bad, but Dangerous: Surveillance as an Ethical Paradox" in Sean Hier & Josh Greenberg, eds, *The Surveillance Studies Reader* (Maidenhead, England: Open University Press, 2007) at 354-368 at 345, "[s]urveillance presents us with constant ethical paradoxes…Surveillance is useful but harmful; welcome but offensive; a necessary evil but an evil necessary. We support surveillance, so long as someone else is in its watchful eye. We find surveillance as something we have to do – even if it is only to protect ourselves or our organizations – but we do not particularly care for it. Hopefully it will hurt you more than it will hurt me…"

children safe and makes our lives more convenient."[12] How and where do you strike a balance between privacy-invasive surveillance practices and the compelling and legitimate goals surveillance seeks to achieve? When does the 'creep factor' cross over to privacy harm worthy of legal protection?[13] These are key questions that need to be addressed since we live in an era of heightened surveillance; some say a "surveillance society."[14]

The study of surveillance has developed largely within sociology, but is emerging as "a sustained multi-disciplinary topic of investigation and theorization,"[15] reflecting the breadth and complexity of surveillance as it has evolved.[16] Although the surveillance potential of emerging technologies is widely acknowledged within this literature,[17] most surveillance research tends to focus on the surveillance capabilities that weaken control over personal information.[18] The primary focus on the data

---

[12] Neil Richards, "The Dangers of Surveillance" (Harvard Law Review, 2013 forthcoming), online: <http://ssrn.com/abstract=2239412>, at 15.

[13] Google Glass, high tech eyewear that delivers features similar to the smartphone, is the most recent product to raise the 'cool' versus 'creep factor' debate. See for example, "Google Glass: Our lives Are Not Reality TV" online: <http://www.readwrite.com/2013/03/04/google-glass-lives-are-not-reality-tv>; "Google Glass: The Creepy Intrusive Privacy Perspective", online: <http://harrisonpensa.com/google-glass-creepy-intrusive-privacy-perspective>. Others say Google Glass is not creepy, just rude, and still others think it is "the greatest thing ever, online: <http://www.realcleartechnology.com/articles/2013/05/09/google_glass_its_rude_422.html>; in the same article, Google chairman, Eric Schmidt, says it is inevitable and society will adapt.

[14] For a historical account of the concept of 'surveillance society', see David Murakami Wood, "The 'Surveillance Society' Questions of History, Place and Culture" (2009) 6:2 European Journal of Criminology 1477.

[15] Sean Hier & Josh Greenberg, "Editors' Introduction: Contemporary Surveillance Studies" in Hier & Greenberg, eds, *The Surveillance Studies Reader* (Maidenhead, England: Open University Press, 2007) at 5.

[16] A deeper sociological enquiry and close examination of the contributions within the multi-disciplines is outside the scope of this project. For overviews of surveillance themes and critiques, see for example, Hier & Greenberg, *ibid*; David Lyon, *Surveillance Studies: An Overview* (Cambridge, UK: Polity Press, 2007;) and Kristie Ball, Kevin Haggerty & David Lyon, eds, *The International Handbook of Surveillance Studies* (New York, Routledge, 2012).

[17] Ball, Haggerty & Lyon, *Handbook of Surveillance Studies*, *ibid*.

[18] See for example, James Rule, *Private Lives, Public Surveillance* (London: Allen Lane, 1973); Oscar Gandy, *The Panoptic Sort: A Political Economy of Personal Information* (Boulder, CO: Westview Press, 1993); David Lyon, *The Electronic Eye: The Rise of the Surveillance Society* (Cambridge: Polity, 1994) and *Surveillance Society: Monitoring Everyday Life* (Buckingham, UK: Open University Press, 2001); Gary Marx, "An Ethics for the New Surveillance" (1998) 14:3 The Information Society 171-186; Kevin Haggerty & Richard Ericson, "The Surveillant Assemblage" (2000) 51:4 British Journal of Sociology 605-622; Stephen Graham & David Wood, "Digitalizing Surveillance" (2003) 23:2 Critical Social Policy; and Elia Zureik et al, eds, *Surveillance, Privacy and the Globalization of Personal Information* (Montreal, PQ: McGill-Queens University Press, 2010).

protection model of informational privacy largely overlooks the implications of the spatial embeddedness of surveillance into our everyday lives. Yet, the privacy issues have moved from atoms (doors, brick walls, and curtains), to bits and bytes (informational technology), only to veer back again to the level of atoms (nano-technology)."[19] It is, therefore, no longer sufficient to limit discussions of privacy to informational privacy or data protection. The embeddedness of the internet of everywhere creates conditions which potentially jeopardize the privacy interests we have; not just those implicating our information, but also those involving our lived embodied spaces.

The overall objective of this chapter is to reassert the relevance and importance of spatial privacy as computing technology becomes embedded in the real world. To achieve this objective, this chapter addresses what surveillance is in a ubicomp environment, the harm arising from surveillance practices, and the spatial dimensions implicated by the enhanced surveillance capabilities. The purpose of this discussion is to lay the foundation for examining the current conceptual and legal basis of spatial privacy in Chapter Three. Further, this chapter serves to inform the development of a new conceptual construct of spatial privacy in Chapter Five.

2. What is Ubicomp Surveillance?

Surveillance, at its social and etymological core is about observation; being seen, watched and monitored. In the traditional sense, surveillance is watching and observing people and spaces with direct physical and visual senses, but increasingly, observation is technologically-mediated.[20] In other words, an embedded device is, in David Lyon's classic description, "the electronic eye."[21] Or, as described by Mark

---

[19] Jeroen Van den Hoven & Pieter Vermaas, "Nano-Technology and Privacy: On Continuous Surveillance Outside the Panopticon" (2007) 32 Journal of Medicine and Philosophy 283, 293.

[20] See for example, Sonia Kaytal, "The New Surveillance" (2004) 54 Case Western Law Review 297; Gary Marx, "Whats' New About the "New Surveillance"?" (2002) 1:1 Surveillance & Society 9-29; David Murkami Wood & C William Webster, "Living in Surveillance Societies: The Normalization of Surveillance in Europe and Britain's Bad Example" (2009) 5:2 Journal of Contemporary European Research 259-273.

[21] Lyon, *The Electronic Eye*, *supra* note 18.

Monmonier, "maps that watch."[22] Although the person or place may be reduced to a digital representation,[23] a real person is being watched on a street, in a coffee shop, at home or any 'place' they visit. Here the notion of cyberspace exists alongside the physical world, converging to form, as discussed in Chapter One, a new hybrid space. In the desktop computing paradigm, cyberspace was largely separated from the physical world, but in the ubiquitous computing paradigm, the physical world and cyberspace are deeply integrated. Thus, as we move through physical space and interact with it, more of our movements and actions will not only be observed, but also captured and recorded in cyberspace. Most commonly today, surveillance is thought of in terms of observation, collection and analysis of information. This is what has now become known as "dataveillance," the systematic use of data systems in the investigations or monitoring of people's actions or communications.[24] All of these dimensions of surveillance have become embedded in the fabric of modern society. The new surveillance is subtle, extensive; intensive yet unobtrusive.

Ubiquitous computing will be everywhere because 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 characteristic of ubicomp, as discussed in Chapter One, is its *invisibility* in the design of everyday lived spaces. Paradoxically, while ubicomp is a powerful means for technological enhancement of vision, it is, literally, visible. You can physically see and touch a device, yet it is 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

---

[22] Monmonier, *Spying with Maps, supra* note 6 at 1.

[23] Daniel Solove, *The Digital Person: Privacy in the Information Age* (New York: New York Press, 2004).

[24] Roger Clarke, "Information Technology and Dataveillance" (1988) 31:5 Comm. of the ACM 498-512.

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 increase. Thus, observation and tracking will result in a greater degree of accuracy, which translates into greater visibility and exposure of people and places. This will enable governments 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.

Now well documented, Bentham's Panopticon, as interpreted by Foucault,[25] has shaped discussions about privacy in the context of surveillance. That the panopticon has enduring metaphorical power is clearly evidenced by its on-going variations to fit the context and to reflect the newest forms of surveillance technology.[26] Yet, developments in technology with enhanced surveillance capabilities have also prompted scholars to rethink Foucault's classic theory. Some question the usefulness of the notion of the panopticon to explain the current surveillance landscape,[27] others see it as a core principle that cannot be ignored, but from which surveillance theory

---

[25] Michel Foucault, *Discipline & Punish: the Birth of the Prison*, translated by Alan Sheridan (New York: Random House, 1995).

[26] See for example, "electronic panopticon": Lyon, *The Electronic Eye*, *supra* note 18; "information panopticon": Shoshana Zuboff, *In the Age of the Smart Machine: the Future of Work and Power* (New York: Basic Books,1988); "super-panopticon": Mark Poster, *The Second Media Age* (Cambridge: Polity, 1995); "participatory panopticon": Kingsley Dennis, "New Instruments of Surveillance and Social Control" Global Research (2008), online: Global Research <http://www.globalresearch.ca/new-instruments-of-surveillance-and-social-control-wireless-technologies-which-target-the-neuronal-functioning-of-the-brain/8263>.; "contemporary urban panopticon": Koskela, "CamEra," *supra* note 6; "societal panopticon": Michael Mehta, "On Nano-Panopticism: A Sociological Perspective" (2002) 54:10 Canadian Chemical News 31); "panoptic surveillance": Vincent Pecora, "The Culture of Surveillance" (2002) 25:3 Qualitative Sociology 345 and Hille Koskela, "Webcams, TV Shows and Mobile Phones: Empowering Exhibitionism" (2004) 2:2-3 Surveillance & Society 199; "panoptic geolocoator": Jonathan Weinberg, "RFID, Privacy, and Regulation" in Simson Garfinkel & Beth Rosenberg, eds, *RFID: Applications, Security, and Privacy* (Boston, MA: Addison-Wesley, 2006); "domestic panopticon": Julie Boesen, Jennifer A Rode & Clara Mancini, "The Domestic Panopticon: Location Tracking in Families" (2010) Proceedings of Ubicomp '10, 12th ACM International Conference on Ubiquitous Computing 65); "embedded panopticon": Jerry Kang & Dana Cuff, "Pervasive Computing: Embedding the Public Sphere" (2005) 62 Wash & Lee LR 93.

[27] See for example, Michael Zimmer, "Book Review of *Theorizing Surveillance: The Panopticon and Beyond*" by David Lyon, ed, (2008) 5:2 Surveillance & Society 203 at 203; Wood, "The 'Surveillance Society'" *supra* note 14.

needs to move beyond,[28] and still others claim the panopticon metaphor has been stretched "beyond recognition in order to account for new technological developments in surveillance."[29] As an analytical tool, the panopticon "might no longer be well suited for understanding the complexity and totality of contemporary surveillance dynamics."[30] For Hille Koskela, the panopticon concept has limitations in the context of contemporary surveillance, but there are strong reasons for keeping it because it helps to understand some of the most vigorous kinds of social control and surveillance, which is important since we cannot escape monitoring, only try to understand it.[31] At the end of day, "a post-panoptic condition does not necessarily imply that we must be anti- or post- Foucauldian" but in the context of ubiquitous computing, it is not a perfect fit to explain surveillance practices.

Visibility is one of the key features in the panopticon model, clearly why it resonated in surveillance studies and privacy discourse, since visibility is an issue of seeing and being seen. However, the invisibility and ubiquity add to "the stealth character" of contemporary surveillance.[32] Rather than being confined by the prison structure of the original panopticon model, ubiquitous surveillance is dispersed and enmeshed across time and space, thus "setting people free from the centralized

---

[28] See for example, David Lyon, ed, *Theorizing Surveillance: The Panopticon and Beyond* (Portland, OR: Willan, 2006) at 12; Clive Norris, "From Personal to Digital: CCTV, the Panopticon and the Technological Mediation of Suspicion and Social Control" in David Lyon, ed, *Surveillance and Social Sorting: Privacy Risk and Automated Discrimination* (London: Routledge, 2002) at 268.

[29] Haggerty & Ericson, "The Surveillant Assemblage", *supra* note 18 at 607-608; Haggerty & Ericson go on to develop an alternative theory which they call 'surveillant assemblage' to describe how various personal information systems extend and intensify processes of social control. See also Kevin Haggerty & Richard Ericson, "The New Politics of Surveillance and Visibility" in Haggerty & Ericson, *supra* note 10 at 4: "surveillance technologies do not monitor people *qua* individuals, but instead operate through processes of disassembling and reassembling. People are broken down into a series of discrete informational flows which are stabilized and captured according to centralized locations to be reassembled and combined in ways that serve institutional agendas. Cumulatively, such information constitutes our 'data double', our virtual/informational profiles that circulate in various computers and contexts of practical application…. The concept of 'surveillant assemblage' points to the disconnected and semi-coordinated character of surveillance…. Hence, while powerful institutions do not control the entire spectrum of surveillance, they are nonetheless hegemonic in the surveillant assemblage to the extent that they can harness the surveillance efforts of the otherwise disparate technologies and organizations."

[30] Kevin D Haggerty, "Tear Down the Walls: On Demolishing the Panopticon" in Lyon, *Theorizing Surveillance*, *supra* note 28 at 38.

[31] Koskela, "CamEra", *supra* note 6 at 307.

[32] van den Hoven & Vermaas, "Nano-Technology and Privacy, *supra* note 19 at 292.

dome."[33] In other words, surveillance in the ubiquitous computing environment departs from the geographic centeredness of a fixed building and moves into, and across, the real world in which we live. This is an important point because, as is argued in later chapters, current legal approaches to protecting spatial privacy need to move beyond the container-thinking of space to adequately protect these interests. In her work on urban surveillance and CCTVs, Hille Koskela identifies space as container, in which, like the panopticon, the camera is detached from the scene it is containing.[34] The camera views the space or place as a contained object and has no interaction on or with it.[35] Moreover, space as container reveals an objectified reality, in which the image, or data subject, displaces reality. It is not unlike a stage space where people pass on and off of the frame of view or stage. The lived world is a two-dimensional projection of the world, void of any human contact, increasing the sense of people as objects in a container.[36] This is not unlike Foucault's observations of the panopticon cells, described as "so many cages, so many small theatres, in which each actor is alone, perfectly individualized and constantly visible."[37] Ubiquitous surveillance is a complex series of interactions with space and experience. By containing and flattening space, it does not take into account the distributed dimensions and practices of our everyday lives.

Further, ubiquitous computing and the surveillance activity it facilitates is not sufficiently explained by the panopticon model because today it is more about technologically-mediated visibility than direct physical visual observation. In other words, visibility is freed from the spatial and temporal properties of the here and now. One no longer has to be present in the same spatial-temporal setting in order to see the

---

[33] *Ibid*; Nicola Green, "On The Move: Technology, Mobility and the Mediation of Social Time and Space" (2002) 65 Law & Contemp Probs 125 at 152.

[34] Koskela, "The Gaze Without Eyes: Video Surveillance and the Changing Nature of Urban Space" (2000) 24:2 Progress in Human Geography 243. In Koskela's view, 'container space' involves an exploration of the consequences of life put on a monitor, contained in the eye of the camera (at 8), 'power-space' on how surveillance affects power interactions (at 13), and 'emotional space' tries to understand the emotional impact of being under surveillance (at 17).

[35] *Ibid* at 7.

[36] *Ibid* at 8.

[37] Foucault, *supra* note 25 at 200.

other person, or observe the action or event. Google Street View, for example, illustrates this point because it is a technology that achieves "sightless vision" where the camera is controlled by a computer.[38] The images that Google Street View captures and manipulates are comprised of real streets with real cars and real pedestrians. Surveillance becomes more amplified when cameras no longer require human control or manipulation. The images gathered within Street View provide a much more realistic experience than the traditional electronic mapping product. These images are intended to provide the experience of actually walking down the street. The resolution of the images allows you to see license plate numbers and to identify the pedestrians captured within the photographs. The images embedded within Street View are effectively capturing a moment in time without the consent of the individuals. There is a distinction between what one sees while walking down the street, fleeting images for the most part, and what Street View captures and embeds within its digital archive. Hence, the privacy implications are more acute.[39]

---

[38] Paul Virilo, *The Vision Machine*, translated by Julie Rose (Bloomington, IN: Indiana University Press, 1994) 134.

[39] See for example, Richard Chirgwin, "Why we should be afraid of Google Street View," *APC Magazine* (11 August 2008), online: APC Mag.com <http://apcmag.com/why_we_should_be_afraid_of_google_streetview.htm>(nude sunbathers being captured); Veronica Lorraine, "Google Cheat View," *The Sun* (31 March 2009), online: The Sun <http://www.thesun.co.uk/sol/homepage/news/article2350771.ece>(cheating spouses). When the service was first launched, the process for requesting that an image be removed was not trivial. Google changed its policy to make removal more straightforward, but has since removed the option to request removal of an image, replacing it by an option to request blurring of an image. Images of potential break-ins, sunbathers, and individuals entering adult bookstores have, however, remained active and these images have been widely republished. Michael Zimmer, "Privacy on Planet Google" (2008) 3 J Bus & Tech 109. See also Office of the Privacy Commissioner of Canada, "News Release: Google contravened Canadian privacy law, investigation finds" (19 October 2010), online: Office of the Privacy Commissioner of Canada Archived News <http://www.priv.gc.ca/media/nr-c/2010/nr-c_101019_e.asp>.

See also *Aubry v Éditions Vice-Versa Inc.* [1998] 1 S.C.R. 591. In this case, 17-year-old Pascale Aubry's photograph was taken while sitting on steps outside a Montreal building and was published in an arts magazine. She sued for invasion of privacy .Quebec recognizes a privacy right in one's image under Article 36 of the *Civil Code of Quebéc*, SQ 1991, c 64 but this action arose prior to this new Civil Code coming into force so was decided under the Quebec *Charter of Human Rights and Freedoms*, RSQ, c C-12, s 5. The Supreme Court of Canada upheld Aubry's right to control her image, even in public. The court argued that because privacy has been recognized to protect autonomy interests, it must include the right to control one's image, which is a part of the control an individual has over his or her identity. One's right to control one's image is an infringement of the person's right to privacy "as soon as the image is published without consent and enables the person to be identified." (at para 53.) Aubry could not complain about simply being observed in public. A public place is one where everyone has a right of physical access and the observation of others is usually incidental to this access. However, the further publication of Aubry's image

3. Visibility and Exposure

In a study of the privacy implications of Facebook, and social networking sites generally, dana boyd begins by offering a simple, yet effective, illustration of the sense of exposure felt where there is unexpected accessibility to the 'self' and our information:

> Imagine that you are screaming to be heard in a loud environment when suddenly the music stops and everyone hears the end of your sentence. Most likely, they will turn to stare at you and you will turn beet red (unless exposure does not bother you). When the music was still chirping away, you were speaking loudly in a room full of people. You felt (and were) protected by the acoustics and you made a judgment about how loudly you should speak based on your understanding of the architecture of the environment. Sure, if someone came closer, they could have overheard you. But you didn't care because (1) you would have seen the person; (2) it is not abnormal to be overheard; and (3) what you were saying would not really matter to them anyhow, right? Most people couldn't hear you even if they were visually proximate. This is security through obscurity. When the music disappeared, the acoustics of the room changed. Suddenly, your voice carried much further than it had previously. Even if there was nothing embarrassing about the content of what you said, you are still startled by the change. Not only did you make a social *faux pas*, but you also lost control over the situation. The color of your face is a direct result of being unexpectedly exposed.[40]

For boyd, what disturbs people when technology makes us more easily accessible is not so much the greater visibility, as that is expected for the most part when in public space, but the sense of exposure experienced.

Gary Marx argues that "a central issue is…what *exposure* means in an age of sense enhancing (and often covertly and remotely applied) surveillance devices, which may, or may not, be widely known about or in common use."[41] Exposure has been

---

was the extension of her observation. This is precisely what technologically-mediated observation accomplishes without human presence or intervention to actually take a photograph.

[40] dana boyd, "Facebook's Privacy Trainwreck" (2008) 14:1 Convergence: Intl J of Research & New Media Tech 13 at 14.

[41] Gary Marx, "Soft Surveillance: The Growth of Mandatory Volunteerism in the Collection of Personal Information – "Hey Buddy Can you Spare a DNA?" in Torin Monahan, ed, *Surveillance and Security: Politics and Power in Everyday Life* (London: Routledge, 2007) at 47. On the issue of soft surveillance and consent, see Ian Kerr et al, "Soft Surveillance, Hard Consent: The Law and Psychology of Engineering Consent" in Ian Kerr, Valerie Steeves & Carole Lucock, eds, *Lessons from the Identity Trail: Anonymity, Privacy and :Identity in a Networked* Society (Toronto, ON: Oxford University Press, 2009) 5-22.

defined in a number of ways; the act of subjecting someone to an influencing experience, abandoning without shelter or protection, presentation to view in an open or public manner, the act of exposing film to light, a picture of a person or scene in the form of a print or transparent slide, recorded by a camera on light-sensitive material, vulnerability to the elements such as heat or cold or wind or rain, aspect regarding light or wind, the disclosure of something secret, the intensity of light falling on a photographic film or plate, or the state of being vulnerable or exposed.[42] Central to these definitions are ideas which are relevant to surveillance.[43] In particular, thinking in terms of 'exposure' helps to explain the harm when surveillance is digital, networked and combined with information.[44] For Julie Cohen, visibility is important in determining accessibility, but the real threats to privacy from visual surveillance are when visual surveillance and data-based surveillance are integrated, enabling both real-time identification of the person and the subsequent searches of stored visual and data-based surveillance records. Therefore, the privacy harm may be visual accessibility or it may be informational accessibility. Although informational and spatial are each important determinants of harm to privacy, it is the combination of these mechanisms, facilitated by the ubiquitous networked environment, that more deeply implicate privacy violations.

Similarly, Ryan Calo maintains that there are two distinct but related categories of privacy harms that may occur as a result of ubiquitous surveillance, what he describes as the subjective and objective.[45] The subjective privacy harm is an internal state, flowing from "the perception of unwanted observation"[46] whereas the objective privacy harm is external to the person, involving "the forced or unanticipated use of information about a person."[47] For Calo, if a person does not know they are being

---

[42] "Exposure," online: Word Reference <http://www.wordreference.com/definition/exposure>.

[43] Kristie Ball, "Exposure: Exploring the Subject of Surveillance" (2009) 12:5 Information, Communication & Society 639-657.

[44] Julie Cohen, *Configuring the Networked Self: Law, Code and the Play of Everyday Practice* (New Haven: Yale University Press, 2012) at Chapter Six, "Privacy, Autonomy and Information."

[45] Ryan Calo, "The Boundaries of Privacy Harm" (2011) 86:3 Indiana LJ 2-31.

[46] *Ibid* at 11.

[47] *Ibid* at 12.

watched, there is a privacy violation, but no harm. The harm is the hurdle that has to be overcome in the context of watching. To overcome, the harm is more than a creep factor, it is the visibility and exposure that necessarily follows from surveillance. For both Cohen and Calo, the privacy harms are the accessibility and observation of information, but also the harm that is "distinctly spatial: that flows from the ways in which surveillance, whether visual or data-based, alters the spaces and places of everyday life."[48]

Gary Marx's border crossing analysis, although focused on information, illustrates how the privacy harms articulated by boyd, Cohen and Calo may arise.[49] For Marx, "central to our acceptance or sense of outrage with respect to surveillance…are the implications for crossing personal borders."[50] Marx identifies four border crossings; physical or natural, social, spatial or temporal, and borders due to ephemeral or transitory effects.[51] First, the real world physical embeddedness and increased connectivity between people, objects and spaces, at best blur natural borders of observability, but more likely penetrate these borders because a new surveillance "is at work that transcends distance, darkness and physical barriers."[52] Moreover, our intuitive expectation that if I cannot see you, then you cannot see me does not apply in the ubicomp context. Also, if physiological sensors are always on and always attached to a person in some way, it is difficult for them to hide their feelings because feelings can be discovered from changes in physiological parameters.[53] This means that facial expressions would no longer constitute a natural border protecting personal feelings.

---

[48] Cohen, *Configuring the Networked Self*, *supra* note 44 at 12.

[49] Gary Marx, "Murky Conceptual Waters: The Public and the Private" (2001) 3:3 Ethics & Information 157-169.

[50] *Ibid* at 158; see also Peter-Paul Verbeek, "Ambient Intelligence and Pervasive Computing: The Blurring of Boundaries Between Human and Technology" (2009) 3 Nanoethics 231.

[51] Marx, *Ibid*.

[52] Colin Bennett, *Privacy Advocates: Resisting the Spread of Surveillance* (Cambridge, MA: MIT Press, 2008) at 16.

[53] See for example, Rosalind Picard, Elias Vyzas & Jennifer Healey, "Toward Machine Emotional Intelligence: Analysis of Affective Physiological State" (2001) 23:10 IEEE Transactions on Pattern Analysis and Machine Intelligence 1175; Carson Reynolds & Rosalind Picard, "Affective Sensors, Privacy and Ethical Contracts" (2004) Proceeding of CHI '04 Extended Abstracts on Human Factors in Computing Systems 1103; Stephen Fairclough, "Fundamentals of Physiological Computing" (2009) 21:1-2 Interacting with Computers 133; and Donald Norman, *The Design of Future Things* (New York: Basic Books, 2007).

Second, social borders, confidentiality and communication expectations are compromised, for example, when 'Mom' learns something confidential via a home smart board, or the human resource department knows you have attended a cancer clinic because of the company GPS monitoring system, or when a person is identified using RFID or biometric technology when entering a store in order to check their credit history which is stored in the database. Social borders might also be crossed when a person at a coffee shop with friends are the target of observation beyond that which might be expected in those circumstances. Third, spatial or temporal borders come with the expectation that parts of our lives can exist in isolation from other parts. Such expectations are violated when ubicomp surveillance systems enable relationships and connections to be made between diverse and seemingly unrelated pieces of data used to create profiles that span space and time. Or, someone may prefer not to convey his or her complete life to everyone, but only different parts of it to different people remaining separated by time (teenage facebook postings) and space (activities outside the employment context). And last, in terms of borders due to ephemeral or transitory effects, assumptions that interaction and communication are not surreptitiously captured, preserved or given new meaning, are potentially crossed by wearable computing devices or mobile devices which allow constant recording of everyday, even mundane, events. The device or application has the advantage of never forgetting anything; any person, activity or statement made is recorded for possible use afterwards.

The ability to rely on these border mechanisms for regulating and sustaining privacy are diminished by the nature of ubiquitous computing and the extent to which it facilitates surveillance. Embedded surveillance networks undermine the pretence that we control our environment or our boundaries within it, a pretence fundamental to the traditional construct of privacy. It is no longer just a question of further eroding the distinction between private and public spaces, or even simply blurring the boundaries of this distinction, but the extent to which ubicomp technologies have almost limitless potential to contravene any reasonable expectations of privacy in private and in public. By permeating boundaries, ubiquitous surveillance alters the

experience of space and place, producing greater transparency and exposure.[54] In turn, "[e]xposure alters the capacity of places to function as contexts within which identity is developed and performed."[55] Privacy invasions now often *feel* different than they did in the past."[56] As Chapter One demonstrated, ubiquitous computing as a "field of operation is by definition total because however discrete ubiquitous technologies may be at their design and inception, their interface with each other implies a domain of action that extends from the very contours of the human body outward to whatever arbitrary space can be equipped with the necessary sensors and effectors."[57] The remainder of this chapter highlights the spatial dimensions implicated by ubiquitous computing and the surveillance practices it facilitates.

4. Spatial Dimensions

4.1 The Body

Already in fairly widespread use, biometrics is the science of identifying people based on their physiological and behavioural characteristics.[58] Biometric technologies, such as eye scans, facial imaging and voice recognition are used to verify identification or pinpoint location. Unlike earlier technologies of identification, biometric systems are seen as more reliable because they do not require someone to have something with them, but rather are part of the person. Tag embedded smart cards, clothing, and

---

54 Cohen*, supra* note 44.

55 *Ibid*.

56 Haggerty & Ericson, *The New Politics of Surveillance & Visibility supra* note 10 at 11; see also Bennett, *Privacy Advocates supra* note 52 at 17, making a similar point that the qualitative changes means that we have less privacy because now we subjectively experience our interactions with institutions and technologies is different.

57 Adam Greenfield, "All Watched Over By Machines of Loving Grace: Some Ethical Guidelines for User Experience in Ubiquitous Computing Settings" (1 December 2004), online: Boxes and Arrows <http://boxesandarrows.com/all-watched-over-by-machines-of-loving-grace-some-ethical-guidelines-for-user-experience-in-ubiquitous-computing-settings-1/>.

58 Anil Jain, Ruud Bolle & Sharath Pankanti, eds, *Biometrics: Personal Identification in the Networked Society* (London: Springer, 2003); Patrick Wang & Svetlana Yanushkevich, "Biometric Technologies and Applications" (2007) Proceedings of 25th IASTED International Multi-Conference: Artificial Intelligence and Applications 226.

generally any 'thing' embedded with an RFID chip further enhance the ability to identify people and things. Some have even voluntarily implanted chips into their bodies or those of their children.[59] Integrating with human-area networking and sensor technology will permit the human body, like intelligent clothing on your body, to be a conduit for electronic transmissions.[60] This creates the potential for an environment described as "uberveillance," an all-encompassing, always-on, always with you, omnipresence surveillance facilitated by technologies that make it possible to embed devices in the human body.[61] Uberveillance is "not on the outside looking down, but on the inside looking out through a microchip that is embedded in our bodies."[62] Conversely, "more technological possibilities will present themselves for the outside world to discover and enter into the human body."[63]

As technology evolves, computers *in* the body mean that technology and the body will be further integrated. [64] While Marshall McLuhan looked at the idea of technology as an extension of our senses, emerging technologies will increasingly become an extension of the human body.[65] When built-in interconnected technology is considered an inseparable part of the body, it "seeks the outside world and pervades it through technology."[66] Moreover, advances in brain technology that let you see what is

---

[59] See for example, Ian Kerr, "The Internet of People: Reflections on the Future Regulation of Human-Implantable Radio-Frequency Identification" in Kerr, Steeves & Lucock, eds, *Lessons from the Identity Trail supra* note 41 at 335.

[60] Kevin Werbach, "Sensors and Sensibility" (2007) 28 Cardozo L Rev 2321.

[61] Michael G Michael & Katina Michael, "Uberveillance: Microchipping People and the Assault on Privacy" (2009) 53:3 Quadrant 85.

[62] "Schott's Vocab: Uberveillance" (4 February 2009), online: New York Times <http://schott.blogs.nytimes.com/2009/02/04/uberveillance/>.

[63] Bert-Jaap Koops & Merel M Prinsen, "Houses of Glass, Transparent Bodies: How New Technologies Affect Inviolability of the Home and Bodily Integrity in the Dutch Constitution" (2007) 16:3 Information & Communication Technology Law 177 at 184.

[64] Ian Kerr, "The Internet of People", *supra* note 59; Ian Kerr, Cynthia Aoki & Max Binnie, "Tessling on My Brain: The Future of Lie Detection and Brain Privacy in the Criminal Justice System" (2008) 50:8 Canadian Journal of Criminology and Criminal Justice 367.

[65] Kevin Warwick, "Identity and Privacy Issues Raised by Biomedical Implants" (2002) 67 IPTS Report 29 and "Wiring in Humans" (Paper delivered at the Conference on 'Safeguards in a World of Ambient Intelligence', Brussels, 21-22 March 2006), online: European Commission Joint Research Centre, Information Society Unit <http://is.jrc.ec.europa.eu/pages/TFS/documents/Deliverable5-ReportonConference.pdf>.; MG Michael & Katina Michael, "Microchipping People: The Rise of the Electrophorus" (2005) 49:3 Quadrant 22.

[66] Koops & Prinsen, "Houses of Glass", *supra* note 63 at 184.

going on inside the brain will allow people to communicate "with other humans merely by thinking to each other."[67] Thus, the use of implants and brain-machine technologies are diminishing the distance between humans and intelligent networks.

Just as the embodied nature of our interaction with computing devices reduces the borders between humans and computers,[68] where the interface or point of contact with computers resides and the extent to which it is visible means the boundary between people and machines will no longer be as clear as when we interacted via the desktop. This boundary moves closer to us, making our interaction with ubicomp systems more intimate and as a result, the self is more accessible, visible and exposed.

4.2 The Home

Although the home is perceived by most as an enclave of privacy and a retreat from the proliferation of surveillance technologies, it provides an almost insatiable market for ubicomp technologies, systems and products targeted at supporting and enhancing the home environment. Take for example, IKEA's "Mother of all Kitchens"[69] which by 2040 will be your personal trainer, dietician, psychologist and lifestyle coach. It will respond to your energy levels, nutritional needs and mood. Or today, Rogers is aggressively marketing its 'Smart Home System' which is "always connected, always close … it's more than just a traditional security system. It's a completely new and innovative application to keeping your home and the people in it safe."[70] Through a touchpad, the brain of the smart home monitoring system provides real time constant monitoring and remote access from anywhere via smart sensors, the eyes and ears of the system, watching movement and automating coffee pots in the home. Or currently used in assisted living facilities, 'intelligent beds' which track the weight of the user, when a resident gets into or leaves a bed, if they are having a quiet sleep, or how many

---

67 Kerr, "Tessling on My Brain", *supra* note 64.

68 See Chapter One, "Embodied Interaction" at p 44.

69 Ikea, "Mother of All Kitchens" (12 August 2010), online: Ikea News Room <http://www.ikea.com/gb/en/about_ikea/newsitem/UK_kitchen_news_release>.

70 Rogers Communications, "Smart Home Monitoring," online: Rogers Home Monitoring <http://www.rogers.com>.

people are in the bed.[71] Similarly, a bed sheet that is able to detect, and broadcast, the number of people lying on it.[72]

In order for the smart home to be an "adaptive and caring environment"[73] it needs to be context-aware, recognize you and your situational context. To do so, it must generate a significant amount of information about the behaviour and lifestyle of the inhabitants. In the ubicomp environment, networked alarm clocks could communicate with the coffee pot, sending a message to switch on or to the toilet seat and towel rail to warm up. Activating the shower might start the toaster. The coffee machine might sense when coffee had been poured and then send a message to the car ignition. In the car, the seat belt might tell the garage door to open, while the garage door turns the central heating down. Nothing in that chain of systems is doing anything more complex than sensing things about their own use and sending basic messages to other gadgets. Out of this simple activity comes a sort of cleverness in the arrangement of our environments serving many important, interesting and genuinely useful purposes, something Vannevar Bush proposed in the 1940's with his information machine 'memex.'[74] What he could not have forseen was how information being gathered could be monitored, with the the 'things' around us telling the world wehre we are and what is going on in our private sphere.

In effect, the perfect smart home "needs to spy on everything that goes on within the walls of the home."[75] In other words, to be intelligent, useful and proactive, the enabling technologies of the smart home influences two important design

---

[71] Natascha Sorenson, C Oestergaard & Birthe Dinesen, "Improving Care of the Elderly with an Intelligent Bed" in M Jordanova & F Lievens, eds, *Global Telemedicine and eHealth Updates: Knowledge Resources, 18-20 April 2012, Luxemburg*, vol 5 (Lucerne, Switzerland: International Society for Telemedicine & eHealth, 2012) 128; Usman Awan, "Wireless Intelligent Bed Sensing System" (B Eng (Hons) Thesis, Massey University, School of Engineering and Advanced Technology, 2009) [unpublished].

[72] This is a reference to electronic textiles or washable computing which are fabrics that can monitor vital signs, generate heat, act as switches or detect pressure: "Threads That Think" *The Economist Technology Quarterly* 377:8456 (8 December 2005) 32.

[73] Anders Albrechtslund, "House 2.0: Towards an Ethics for Surveillance in Intelligent Living and Working Environments" in (2007) Proceedings of CEPE 2007, International Conference of Computer Ethics: Philosophical Enquiry 7.

[74] Vannevar Bush, "As We May Think" *The Atlantic* (July 1945) <http://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/3881/>.

[75] *Ibid* at 8.

parameters, the ability to track and the ability to monitor. Thus, its underlying technologies necessarily implicate privacy. The people, the home and things inside it become transparent when "walls and curtains will no longer protect it from prying eyes and ears."[76] For example, some smart appliances are capable of communicating within the home to other devices, but also to the outside world about what is going on inside the home,[77] while technologies now commonly used by law enforcement are capable of seeing through walls.[78] The new surveillance will be aided not by the human senses, a telephoto lens, or even thermal imaging, but by, for example, coffee pots and bed linens.[79]

It is not just technologies that can penetrate the home as traditionally understood, but it is also the way in which technologies are expanding the private places of interaction outside the home. Cell phones, laptops, tablets, wireless networks, and now ubiquitous computing, enable unlimited mobile connectivity. Activities previously available solely within the home are now available anywhere, anytime. Technology-mediated interaction takes place on buses, in cars, in classrooms, in shopping malls and on streets. Coffee shops, libraries, parks and airports are populated with connected users who do work, banking, research, shopping and socializing. Traditionally home-based tasks and activities can now be done anywhere on a mobile device and increasingly, social and intimate interactions occur via the devices we carry with us, or on the device as we move across spaces outside the home. The result is not only a lifestyle that encourages mobility and interconnectivity, but also the idea that one can feel or be 'at home' while mobile – a mobile home of sorts.[80] As soon as the cell

---

[76] Koops & Prinsen, "Houses of Glass, Transparent Bodies", *supra* note 63 at 180.

[77] See for example, Rossilin Robles and Tai-hoon Kim, "Applications, Systems & Methods in Smart Home Technologies" (2010) 15 International J of Advanced Science and Technology 37-48; Michael Friedewald et al, "Perspectives of Ambient Intelligence in the Home Environment" (2009) 22:3 Telematics & Informatics 221-238..

[78] Vanmala Hiranandani, "Under-Explored Threats to Privacy: See-Through-The-Wall Technologies and Electro-Magnetic Radiations" (2010) 8:1 Surveillance & Society 93-98.

[79] The phrase 'new surveillance' was first used by Gary Marx and subsequently applied in a series of articles, online: <http://www.mit.edu/gtmarx/www/garyhome.html>.

[80] Paul Levinson, *Cellphone: The Story of the Most Mobile Medium and How it Transformed Everything* (New York: Palgrave MacMillan, 2004).

phone began connecting to the Internet, it became "a home away from home for communications, a mobile home, a traveling medium of media."[81] As elaborated on in later chapters, this effectively alters the traditional understandings of the home.

4.3 The Public Sphere

Surveillance today is about monitoring everyday life and targets everyone, not just those under suspicion, in which there is a systematic attention to even the routine and mundane personal aspects of an individual's life.[82] The ultimate convergence issue is the trend towards pervasive computing and the internet of everything, in which "the internet does not only link computers and communication technologies, but potentially any of our daily surrounding objects."[83] The possibility is a "digitally saturated world" in which surveillance sensors are placed or carried virtually everywhere, in clothes, money, household appliances and products, and cars, for example, with the potential to continuously and routinely watch people and gather information.[84] It can be difficult for citizens to appreciate the privacy implications of routine surveillance. The attitude 'if I've got nothing to hide, I've got nothing to worry about' is prevalent, particularly where the surveillance is justified for public interest reasons.[85] Moreover, there is no longer the need to surreptitiously install tracking devices on persons, vehicles or objects because increasingly people carry or use tracking devices voluntarily in their everyday lives.

The surveillance no longer refers to fixed spaces, but instead now exists in a world of flows.[86] The means of communication are increasingly mobile and people on

---

81 *Ibid* at 53.

82 David Lyon, *Surveillance Society*, *supra* note 18; Colin Bennett & Priscilla Regan, "Surveillance & Mobilities" (2004) 1:4 Surveillance & Society 449; Robert O'Harrow, *No Place to Hide: Behind the Scenes of Our Emerging Surveillance Society* (2005); James Rule, *From Mass Society to Perpetual Contact: Models of Communication Technologies in Social Context* (New York: Cambridge University Press, 2002).

83 Yves Punie et al, "Ambient Intelligence: Highlighting the Risks and Vulnerabilities" (November 2005) A report of the SWAMI consortium to the European Commission, November 2005 at 6, online: <http://swami.jrc.es>.

84 *Ibid*.

85 Daniel Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (New Haven: Yale University Press, 2011) 21-32.

86 Manuel Castells, *The Rise of the Network Society* (Oxford: Blackwell, 1996) at 376.

the move will make it difficult to evade surveillance.[87] 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 surveyed, but instead each becomes a point on the flow of surveillance."[88] 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 shops, to taking a walk down our neighbourhood street, all these movements and 'flows' are subject to scrutiny.[89] The objects we use or carry with us, in turn, become tools for surveillance. Movement 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, even "the street itself seems to have evolved into a sensory apparatus."[90]

As computing technology moves beyond the desktop into the sites and situations of everyday life, embedding the public sphere shifts the emphasis from abstract data processing to the concrete physical space of the entire urban landscape. In the public sphere, ubicomp will make us more visible and thus more vulnerable to the harm that it causes because "[w]ho looks at us, how, how long, and for what purposes matter."[91] For example, "[w]hen technology enables the government to stare with an ever-vigilant and suspicious eye, the boundaries of the self may partly dissolve, reconstructed in the image chosen by Leviathan…Regulation [of this technology] preserves the idea of a diverse, noisy America, where citizens are free to get lost in the crowd and where their sense of self stems from their chosen affiliations and actions

---

87 Lyon, "Surveillance Studies," *supra* note 11 at 3; Haggerty & Ericson, "The Surveillant Assemblage," *supra* note 18 at 607, claiming that "there will be no place on earth where an ordinary person will be able to avoid surveillance."

88 Bennett & Regan, "Surveillance and Mobilities," *supra* note 82 at 453.

89 *Ibid.*

90 William Gibson, "The Road to Oceania" *New York Times* (25 June 2003), online: New York Times Opinion <http://www.nytimes.com/2003/06/25/opinion/the-road-to-oceania.html>.

91 Andrew E Taslitz, "The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions" (2002) 65:2 Law & Contemporary Problems 125 at 171.

rather than from the all-seeing gaze of the state."[92] What is at stake here is a loss of anonymity and what is troubling about losing anonymity is that it subjects us to the gaze, impairing aspects of individuality that are, or should be, protected in a free and democratic society.[93] For Alan Westin, anonymity occurs when the individual is in public spaces or performing public acts but still seeks, and finds, freedom from identification and surveillance.[94] He may be riding a subway, attending a ball game, or walking in the streets; he is among people and knows that he is being observed, but does not expect to be subject to systematic observation or be personally identified. In this state the individual is able to merge into the "situational landscape."[95] Therefore, it is not simply that we are identified by others that creates the loss of privacy, but the fact that the identification subjects us to a kind of inhibiting standard of public or social norms; in other words, the inhibiting effects of being subject to observation. Even though we are generally observed by others when in public, as long as we are strangers to those people, and the observation is generally fleeting, we are not subject to the same kinds of norms. Yet, the underlying concern remains observation and exposure from which visibility flows.

It is, however, not only the nature of the activities observed by surveillance that makes it so troubling, but the extent to which it changes the nature of the public space and deprives it of the qualities that have sustained it as a site for anonymous, private and spontaneous action.[96] In other words, anonymity is particularly vulnerable in the

---

92 *Ibid* at 171-172.

93 Lisa Austin, "The Privacy Interests at Stake in Public Activities" Innovate (Spring 2006) at 18, online: <http://www.law/utoronto.ca/documents/publications/Innovate06.pdf>. See also Jeffrey Reiman, "Driving to the Panopticon: A Philosophical Exploration of the Risks Posed by Highway Technology of the Future" in Beate Rossler, ed, *Privacies: Philosophical Evaluations* (Stanford, CA: Stanford University Press, 2004) 194-214, at 201-206, discussing how surveillance assaults human dignity and changes behavioural patterns, thereby reducing self-determination.

94 Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967).

95 *Ibid* at 31.

96 Marc Jonathon Blitz, "The Dangers of Fighting Terrorism with Techcommunitarianism: Constitutional Protections of Free Expression, Exploration and Unmonitored Activity in Urban Spaces" (2004) 32 Fordham Urb LJ 677; Timothy Zick, "The First Amendment and Networked Public Places" (2007) 59 Florida LR 1; Daniel Solove, *Understanding Privacy*, (Cambridge, MA: Harvard University Press, 2008) at 108, citing a privacy harm in this regard as dampening public discourse, chilling behaviour and refraining people from expressing themselves freely.

ubicomp environment. It was less of a concern with previous generations of technologies because they were not as pervasively and invisibly embedded in the physical world – in both private and public spaces. Nor did technology travel with us across these spaces as they do today. We were relatively free to be anonymous on the street, at the store, in a park, at an airport and even in a large university class. There were physical barriers or social norms limiting surveillance. Section 8 under the *Canadian Charter of Rights and Freedoms* [97] purports to recognize a reasonable expectation of spatial privacy and if so, what spaces or places can we exercise that right? Moreover, ubicomp technologies are reconfiguring the landscape with the potential to seriously minimize spaces and places to be anonymous and diminish the ability to carry out our private activities in those spaces. This is illustrated by the mass surveillance systems in the cities of New York and London.[98]

In 2007, New York City began its "Manhattan Security Initiative" that, when completed, will include a network of some 3000 television cameras implemented to ensure public safety and security and to detect, deter and prevent potential terrorist

---

[97] Section 8 provides that "[e]veryone has the right to be secure against unreasonable search or seizure": Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11 [Charter].

[98] New York and London's surveillance systems are reminiscent of the scenarios described by David Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* (Cambridge, MA: Perseus Books, 1998). Brin articulates his vision of two cities, one transparent and the other a surveillance society. Both, he said, would be thoroughly modern containing "dazzling technological marvels" yet "suffer familiar urban quandaries of frustration and decay." (at 5). They could be Copenhagen, Vancouver, Dubai, Chicago or Sydney. The precise location did not matter. What did matter would be that visitors to these future cities would notice something starkly similar about both. Street crime would be conspicuous by its absence. It would have all but vanished because peering down from "every lamppost, rooftop, and street sign… tiny cameras, panning left and right" would watch over the inhabitants of both cities "surveying traffic and pedestrians, observing everything in open view."(at 3-4) But City Number One was not unlike the dark portrayal in George Orwell's *1984*, whereas City Number Two was transparent. The thing that so disturbed Brin over a decade ago, the ubiquity of cameras may be materializing in an updated version of Brin's vision: ubicomp. Cameras might even be rendered irrelevant by the range of more sophisticated technologies. London and New York seem much closer to Brin's vision and in future cities, instead of cameras on top of each lamppost, there is a near invisible network of wireless frequencies where objects, people and spaces can be located and monitored, found and logged easily. They are places where the urban and domestic infrastructures are embedded with a sophisticated network of traceable things and people. Brin's 'transparent society' is the 'ubiquitous networked society,' our future cities of glass: Corning, "A Day Made of Glass," online: YouTube <http://www.youtube.com/watch?v=6Cf7IL_eZ38>; Google, "Project Glass," online: <http://www.youtube.com/watch?v=9c6W4CCU9M4>. Your movements are watched, not by the use of crude cameras, but by embedded chips, transmitting wirelessly, connecting in real time to systems that watch endlessly.

activities.[99] This network spans close over a two square mile area. The system also includes chemical, biological and radiological sensors intended to detect potential terrorist threats. Some cameras are equipped with 'see-through' technology that can detect when an individual is carrying a gun. It also includes license plate readers, which can zoom in on license plates. The system also integrates private security technologies so that surveillance is not limited to public areas. The New York surveillance system is not new and was based on the "Ring of Steel" system that surrounds London.[100] In greater London, "when Britains leave their homes what will be remarkable is if their presence is not seen, their behaviour is not monitored and their movements not recorded by the omni-presence of the cameras."[101]

Most recently, in response to the horrific bombings in Boston, New York Mayor Michael Bloomberg has called for increased surveillance.[102] More visibility and less privacy is the message. Bloomberg said, "[i]ts not a question of whether it is good or bad, I just don't see how you can stop it."[103] And United States Circuit Court of Appeals Justice Richard Posner agrees.[104] Like Bloomberg, Posner says people's attitudes about privacy have to change and need to take second place to security. Posner argues there is no privacy in public so why even worry about it in the ongoing national security battle. For privacy advocates, as the technology matures, more public surveillance will allow police to monitor all of our movements in public linked to our real identities, not just to our anonymous faces.[105] According to Daniel Solove, intrusions of this kind, into

---

[99] New York Police Department, "Press Release: Midtown Manhattan Security Initiative", online: NYPD <http://www.nyc.gov/html/nypd/html/pr/pr_2010_midtown_security_initiative.shtml>.

[100] Jon Coaffee, "Rings of Steel, Rings of Concrete and Rings of Confidence: Designing Out Terrorism in London" (2004) 28:1 Intl J of Urb & Reg Research 201. There are no Canadian cities with surveillance systems of this magnitude, although Toronto's billion-dollar security system for the 2010 World Leaders Conference might be characterized as a smaller version of the 'ring-of-steel'.

[101] Coaffee, *ibid* at 203.

[102] "Security Cameras Everywhere" New York Daily News (April 2013), online: <http://www.nydailynews.com/new-york/Bloomberg-new-york-eventually-surveillance-city-article-1.1296103#ixzz2RxrsxDk7>.

[103] *Ibid.*

[104] "Privacy Overrated" New York Daily News (April 2013), online: <http://www.nydailynews.com/opinion/privacy-overrated-article-1.1328656?print>.

[105] Neil Richards, "Surveillance State no Answer to Terror" (April 2013), online: <http://www.cnn.com/2013/04/23/opinion/richards-surveillance-state/index.html>.

one's life in non-traditional environments, "disturbs the victim's daily activities, alters her routines, destroys her solitude, and often makes her feel uncomfortable and uneasy."[106]

5. Conclusion

In February 2013, the Ontario Provincial Police approved a plan to begin using drones for surveillance purposes.[107] Drones, or unmanned aerial vehicles (UAVS), are aircraft either controlled by 'pilots' from the ground or increasingly, operated autonomously. While drones have been in use for some time, their use to date has largely been limited to military purposes or as an investigative tool for accident sites.[108] In other words, essentially benign purposes such as accident reconstructions and crime scene surveys. Law enforcement agencies say that the use of drones for surveillance purposes will save time, money and potentially save lives,[109] clearly legitimate objectives. However, many surveillance technologies begin in the military environment or in the context of safety prevention, but move into the civilian realm, GPS being the most obvious example.[110] It is this issue of "function creep"[111] which raises further privacy concerns, both spatial and informational. When walking into the bank most of us today know that there is a risk of being caught on closed-circuit television cameras, or even at the ATM banking machine, many people are now aware of being watched and our transactions being tracked from that location. However, a

---

106 Daniel Solove, *Understanding Privacy*, *supra* note 96 at 162.

107 Jennifer Quinn, "Police drones sparks debate over personal privacy" *The Star* (5 February 2013), online: thestar.com <http://www.thestar.com>. See also, Sigrid Forberg, "Taking to the skies: New tool facilitates investigations" (2012) 74:1 Gazette, online: Royal Canadian Mounted Police <http://www.rcmp-grc.gc.ca/gazette/vol74n1/trends-dernierestendances-eng.htm>.

108 Quinn, *ibid*; drones were also used after the Elliot Lake Shopping Mall collapse, in disaster zones to search for missing people, and during the London 2012 Olympics: Dave Zirin, "Drones, missiles and gunships: Welcome to the 2012 London Olympics" *The Star* (21 May 2012), online: thestar.com <www.thestar.com>.

109 Quinn, *ibid*.

110 Monmonier, *Spying With Maps*, *supra* note 6; and JK Peterson, *Understanding Surveillance Technologies: Spy Devices, Privacy, History and Applications*, 2nd ed (Boca Raton, FLA: Taylor & Francis, 2007).

111 Function creep refers to the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, especially when this leads to a potential invasion of privacy. See for example, David Lyon, *Identifying Citizens: ID Cards as Surveillance* (Oxford: Polity Press, 2009); Mark Andrejevic, *iSpy: Surveillance and Power in the Interactive Era* (Lawrence, Kansas: University of Kansas Press, 2004).

drone, thousands of feet in the air, can be watching us remotely and without our knowledge as we carry out our everyday lives. This type of surveillance provides yet another layer of surveillance along with thermal imaging of the home, GPS vehicular tracking, and location-aware cell-phones. The seamless integration of ubiquitous computing enhances and extends what drones do from the sky, the ability to locate and track people and things in the real physical world anywhere, anytime, accurately, continuously and in real time. Canadian drones, according to law enforcement, are only looking at areas that would be considered public by the courts, thus permissible without legal authorization.[112] Yet, it is this type of activity by law enforcement, without a warrant, that section 8 of the *Canadian Charter* originally sought to curtail in order to protect a person's reasonable expectation of privacy.[113]

Ubiquitous computing poses unique challenges by virtue of its potential to create a "comprehensive surveillance network, covering an unprecedented share of our public and private life."[114] What emerges is not just a new set of concerns for data protection and informational privacy. The seamless integration of technologies, physically and invisibly, into the real world of our everyday lives, more directly and more pervasively, compromises the spatial dimensions of privacy. This potential to be caught within a web of constant accessibility, visibility and exposure challenges our fundamental ideas about personal space, private places, boundaries, and the privacy expectations that accompany them. These issues necessitate revisiting the conceptual underpinnings of spatial privacy, examining the extent to which spatial privacy is protected in law and assessing whether current approaches adequately address these challenges. This examination is taken up in Chapter Three.

---

[112] Quinn, *supra* note 107.

[113] *Hunter v Southam Inc*. [1984] 2 SCR 145.

[114] Jurgen Bohn et al, "Living in a World of Smart Everyday Objects – Social, Economic and Ethical Implications" (2004) 10:5 Human & Ecol. Risk Assess. 763 at 771.

CHAPTER THREE

THE PRIVACY LANDSCAPE: THEORY AND LAW

The door refused to open. It said, 'Five cents, please.' He searched his pockets. No more coins; nothing. 'I don't have to pay you.' 'I think otherwise,' the door said… It sounded smug… From the drawer beside the sink Joe Chip got a stainless steel knife; with it he began systematically to unscrew the bolt assembly of his apt's money-gulping door. 'I'll sue you,' the door said as the first screw fell out.

Philip K. Dick, *Ubik* (1969)

1. Introduction

Police reliance on GPS technology to gather crucial evidence by electronically tracking suspects' vehicles provide unique and valuable investigative opportunities.[1] However, when GPS technology was installed by Washington, DC police on suspected drug dealer Antoine Jones' jeep without a valid warrant, and monitored for one month, the United States Supreme Court decided the police violated Jones' constitutional right to be free from unreasonable search and seizure.[2] While the outcome may have been

---

[1] For example, in the 2004 trial of Scott Peterson for the murder of his wife Laci Peterson, a Global Positioning System (GPS) unit attached to Scott Peterson's vehicle provided the evidence police needed to tie Peterson to the murder: *The People of the State of California v Scott Lee Peterson*, Superior Court of the State of California for the County of Stanislaus, Case No. 1056770. See also "Judge Allows GPS Evidence in Peterson Case" *CNN.com* (17 February, 2004), online: CNN.com <http://www.cnn.com/2004/LAW/02/17/peterson.trial/index.html>. And in 2008, Washington, D.C. area police were able to catch a rapist by installing GPS technology to his vehicle and tracking his movements until he led police to a wooded area where he was about to attack another victim: Ben Hubbard, "Police Turn to Secret Weapon: GPS, Device" *Washington Post* (13 August 13, 2008), online: <http://Washingtonpost.com>.

[2] *United States v Jones*, 565 US 132 S Ct 945 [*Jones*]. The United States Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause,

welcomed by privacy advocates, the decision ultimately raises more uncertainty in the context of government searches.

In *Jones,* three opinions concluded that the government's action was a search in violation of the Fourth Amendment protection under the United States Constitution.[3] Writing for the majority, Justice Scalia found the government's act of physically attaching the GPS device to the car was a trespass on the defendant's property.[4] For Justice Alito, GPS tracking was a search, but the risk GPS posed was a loss of privacy, not property; he took issue with the "long-term" tracking of the defendant.[5] And Justice Sotomayor agreed that the physical trespass of attaching the GPS device was a violation of the Fourth Amendment, as it "reflects an irreducible constitutional minimum," but since "physical intrusion is now unnecessary to many forms of surveillance" the existing safeguards no longer necessarily "constrain abusive law enforcement practices."[6] This is particularly prolific when you consider 'smart cars' currently on display at auto shows. Over the next decade, cars will be connected and equipped with sensors and onboard computers replacing external GPS devices.[7] Beyond the vehicle context, as the previous chapters described, people, places and things everywhere will be connected and equipped with surveillance enhanced

---

supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." US Const, Amend IV.

Under the Canadian equivalent, "[e]veryone has the right to be secure against unreasonable search or seizure": *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11, s 8 [*Charter*].

3 *Jones*, *ibid* at 948-949 (majority opinion). The police had initially obtained a warrant to place the GPS device, but installed the device after the warrant expired.

4 *Ibid* at 949-950. Justice Scalia cited historical precedent of people being secure in their "persons, houses, paper and effects" from unreasonable searches and went on to note that although *Katz v United States*, 389 US 347 (1967) [*Katz*], changed the test for applying Fourth Amendment protection, it in no way repudiated this basic principle. In *Katz,* United States Supreme Court Justice Harlan (in)famously articulated the reasonable expectation of privacy test in the context of government searches. Justice Scalia's majority opinion in *Jones*, therefore, introduces "a new twist…on search doctrine that must now be understood as including two distinct parts: the *Katz* test and the trespass test." Orin Kerr, "The Curious History of Fourth Amendment Searches" (Supreme Court Review, 2013 forthcoming), online: <http://ssrn.com/abstract+2154611>.

5 *Ibid* at 964 (Alito, J. concurring).

6 *Ibid* at 955-956.

7 "Smarter on the way" 19th World Congress on Intelligent Transport Systems (25-26 October 2012), online: 19th ITS World Congress <http://2012.itsworldcongress.com/content>.

technologies, thus potentially extending the reach of government searches to our everyday movements whether we are in a vehicle or not.

Jones is the most recent case in the context of search and seizure law to highlight the increasing tension between the newest technology and our expectation of privacy. While none of the American Justices in *Jones* sided with the government, critical questions are left open. For example, what is the reasonable expectation of privacy in a world in which cell phones have GPS, public spaces are camera-equipped and computing is being embedded in everyday things, people and places? In Justice Alito's view, "[t]he best we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated. Under this approach, a relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable." Thus, Justice Alito may have been asking the right question, whether GPS tracking violated today's reasonable expectation of privacy and not those of another era, but "[n]ew technology may provide increased convenience or security at the expense for privacy, and many people may find that worthwhile." Thus, the standard Justice Alito's applied is problematic. Focusing on public expectations of privacy means that our rights change when technology does, reinforcing the circular nature of the reasonable expectation of privacy test. But more troublesome is Justice Scalia's 'trespass theory' grounded in property law principles and hinging on physical intrusion. Since much of the *Jones* case ultimately comes down to a distinction between 'inside' and 'outside' – or the underlying assumption of privacy protection resting on the private-public divide – is an electronic tracking device permissible for "short-term" surveillance provided there is no physical trespass and provided it is not used inside a house?[8] If so, how does this account for the changing nature of technologies when

[8] For the Supreme Court of Canada in *R v Tessling,* [2004] 3 SCR 432 [*Tessling*], the 'inside' – 'outside' analysis was central to its finding that police using Forward-Looking Infra-Red (FLIR) technology to get information about heat emanating "off-the-wall" of the accused's house, from which they could draw inferences about activities that were likely going on, did not violate section 8 of the *Charter*. In other words, although operating 'outside' the house, the police could obtain sensitive information about 'inside' the property without a warrant. Although FLIR technology may not be as invasive as GPS technology,

emerging surveillance practices do not necessarily engage trespass and, increasingly, occur outside the house in the lived spaces of our everyday lives? This raises the issue of spatial privacy: its nature and its protection in law.

Privacy concerns seem to go hand in hand with new technologies. Ideas about privacy, at least since the 19th century, are closely associated with technology and social change, whether it be the development of printing, changes in housing, the invention of the portable camera, the rise of popular journalism, the creation of computer databases or the rise of the internet. All, to a greater or lesser extent, have prompted concerns, and a rethinking of our attitude toward privacy, because new technologies reformulate the character of the privacy invasion and test the parameters of the concept. Ubiquitous computing represents yet another technology shift influencing our understanding of what privacy is and how it ought to be protected. The automated processing of personal data using computers and the creation of massive database technology beginning in the 1960's changed the face of privacy. The focus of theoretical and legal discourse on privacy shifted from the protection of the classic forms of privacy, such as the body and the home, to the protection of personal information. While many of the larger questions with respect to the data protection model of information privacy have been addressed, spatial privacy has largely been ignored. The difference in focus may be explained by the need to protect individuals against the risks that come along with people's vulnerabilities as a result of the particular technological developments. For example, the rise of mass media, databases and the personal computer influenced an understanding of privacy in terms of access to data or information.

Faced with recurring claims of privacy's demise,[9] or precisely because of them, concern, fascination and debate continues because most people would agree that

---

Tessling demonstrates how technology potentially renders the inside/outside distinction irrelevant. See *Kyllo v United States* 121 S. Ct 2038 (2001) at para 19, where Justice Scalia makes the distinction between "off the wall" technologies (those that detect or observe only the exterior of a building) and "through-the-wall" technologies (those that can see through walls).

[9] See for example, Reg Whitaker, *The End of Privacy: How Total Surveillance is Becoming a Reality* (New York: New Press, 1999); Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* (Sebastopol, CA: O'Reilly & Associates, 2000); Jeffrey Rosen, *The Unwanted Gaze: The Destruction of*

privacy is an important value. While some are skeptical,[10] most privacy scholars contend that privacy promotes freedom and autonomy,[11] personhood and the creation of self,[12] human dignity,[13] intimacy and relationships,[14] democracy,[15] and the rejection of totalitarianism.[16] Others argue the social value of privacy.[17] The Supreme Court of

---

Privacy in America (New York: Random House, 2000); Michael Froomkin, "The Death of Privacy" (2000) 52 Stan L Rev 1461; Ben Hubbard, "Police Turn to Secret Weapon: GPS, Device" *The Washington Post (*13 August 2008), online: The Washington Post <http://www.washingtonpost.com>.

[10] For example, those who dismiss privacy as simply protecting property interests: see for example, Judith Jarvis Thomson, "The Right to Privacy" (1974) Phil & Public Affairs 4 and Richard S Murphy, "Property Rights in Personal Information: An Economic Defense of Property" (1996) 84 Geo LJ 2381; and those dismissing privacy as promulgating subordination of, and violence to, women by men: see for example, Catherine MacKinnon, *Toward A Feminist Theory of the State* (Cambridge, MA: Harvard Univ Press, 1989); Elizabeth Schneider, "The Violence of Privacy" (1991) 23 Conn L Rev 973 and Reva Siegal, "The Rule of Love: Wife Beating as Prerogative and Privacy" (1996) 105 Yale LJ 2117. Other feminist scholars challenge assumptions within the privacy paradigm, but do not reject privacy outright, instead seeing the usefulness of a concept of privacy or the value of privacy itself in the human life: see for example, Carole Pateman, "Feminist Critiques of the Public/Private Dichotomy" in Carole Pateman, *The Disorder of Woman: Democracy, Feminism and Political Theory* (Palo Alto, CA: Stanford Univ Press, 1989) 118; Ruth Gavison, "Feminism and the Public/Private Distinction" (1992) 4:1 Stan L Rev 4; Anita Allen, *Uneasy Access: Privacy for Women in a Free Society* (Savage, MD: Rowman & Littlefield, 1988) and *Unpopular Privacy* (New York: Oxford Univ Press, 2011). For an overview of these views, see Jena McGill, "What Have You Done for Me Lately? Reflections on Redeeming Privacy for Battered Women" in Ian Kerr, Valerie Steeves & Carole Lucock, eds, *Lessons from the Identity Trail: Privacy & Identity in a Networked Society* (Toronto, ON: Oxford University Press, 2009) 157. Others contend privacy can be socially detrimental by facilitating misrepresentation of one's self: see for example, Richard Epstein, "The Legal Regulation of Genetic Discrimination: Old Responses to New Technology" (1994) 74:1 B U L Rev 13; or by giving individuals the power to conceal information about themselves that others might use to disadvantage: Richard Posner, *The Economics of Justice* (Cambridge, MA: Harvard Univ Press, 1981) 271.

[11] See for example, Beate Rossler, *The Value of Privacy,* translated by RDV Glasgow (Cambridge, UK: Polity Press, 2005); Louis Henkin, "Privacy & Autonomy" (1974) 74 Colum L Rev 1410; Ruth Gavison, "Too Early for a Requiem" (1992) 43 S C L Rev 437; Julie Cohen, *Configuring the Networked Self: Law, Code and the Play of Everyday Practice* (New Haven, CT: Yale University Press, 2012) at 107.

[12] The term 'personhood' has been attributed to Paul Freund who defined it as the "attributes of an individual which are irreducible in his selfhood" and related to privacy and autonomy: J B Craven, "Personhood: The Right to Be Let Alone" (1976) Duke LJ 699 at 705 n 15. See also for example, Jeffrey Reiman, "Privacy, Intimacy & Personhood" (1976) 6 Phil & Public Affairs 26; and Stanley Benn, "Privacy, Freedom & Respect for Persons" (1971) 13:1 Nomos 26.

[13] See for example, Edward Bloustein, "Privacy as an Aspect of Human Dignity" (1964) 39 NYU L Rev 962; David Matheson, "Dignity & Selective Self-Presentation" in Kerr, Steeves & Lucock*, supra* note 10 at 319; and Helen Nissenbaum, *Privacy in Context: Technology, Policy & the Integrity of Social Life* (Stanford, CA: Stanford Univ Press, 2010).

[14] See for example, James Rachels, "Why Privacy is Important" (1975) 4 Phil & Public Affairs 323; Julie Inness, *Privacy, Intimacy and Isolation* (New York: Oxford University Press, 1992); Reiman, "Privacy, Intimacy & Personhood," *supra* note 12.

[15] Jeffrey Reiman, "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Information Technology of the Future" in Bette Rossler, ed, *Privacies: Philosophical Evaluations* (Stanford, CA: University of Stanford Press, 2004) 194.

[16] Jeb Rubenfeld, "The Right to Privacy" (1989) 102 Harv L Rev 737.

Canada has grounded privacy "in physical and moral autonomy – the freedom to engage in one's thoughts, actions , decisions"[18] and emphasized that "[t]he protection of privacy is a fundamental value in modern, democratic states"[19] worthy of constitutional protection for that reason alone, but having "profound significance for the public order" as well.[20] Yet, while we may care about privacy and the values it purports to protect, delineating a coherent conceptual basis and legal model for privacy protection has become something of a holy grail. In the context of spatial privacy, legal approaches have tended to rely on traditional exclusionary theories of privacy which, under the current territorial model of spatial privacy, are implicitly proprietary. The shift to an informational analysis has further marginalized spatial privacy interests.

This chapter canvasses the conceptual and legal privacy landscape. It sets out first the conceptual foundations of privacy, the focus of which is on those theories that inform spatial privacy: non-intrusion and inaccessibility. Informational privacy is also considered to the extent that it overlaps with the spatial dimensions of privacy. It is not the aim here to offer a new theory of privacy. Rather, the descriptive overview provides the conceptual basis for the analysis of the hierarchical categorization of privacy interests as bodily, territorial and informational.[21] The remainder of this

---

17 See for example, Priscilla Regan, *Legislating Privacy* (Chapel Hill: University of North Carolina Press, 1995); Arthur Cockfield, "Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies" (2007) 40 UBC L Rev 41; Valerie Steeves, "Reclaiming the Social Value of Privacy" in Kerr, Steeves & Lucock, *supra* note 10 at 191; and Daniel Solove, *Understanding Privacy* (Cambridge, MA: Harvard University Press, 2008).

18 *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403 at para 65 [*Dagg*]. See also *R v Plant*, [1993] 3 SCR 281 at para 17 [*Plant*], in which the Court recognized the values protected under section 8 are "dignity, integrity and autonomy."

19 *Ibid*.

20 *R v Dyment*, [1988] 2 SCR 417 at para 17 [*Dyment*].

21 The 'zones' terminology to classify the dimensions of privacy has been used by the Supreme Court of Canada in recognizing that privacy claims may attach to bodily, territorial and informational privacy interests. See for example, *Dyment, supra* note 20, *Tessling*, *supra* note 8 and *R* v *Patrick* [2009] 1 SCR 579 [*Patrick*]. These categories basically align with Beate Rossler's treatment of privacy as local, informational and decisional, *supra* note 11, although Rossler's third category falls more properly within section 7 of the *Charter* which provides, "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." See for example, *R* v *Morgentaler*, No 2, [1988] 1 SCR 30 (the right to liberty contained in section 7 should be construed broadly to include a right to make private decisions); and *Rodriquez* v *British Columbia (Attorney-General)*,

chapter examines the reasonable expectation of privacy standard as it has been applied under section 8 privacy jurisprudence through the zonal analytical framework. As this discussion will show, current approaches to protecting privacy do not effectively answer the questions relating to spatial privacy in the context of technology-mediated surveillance. Chapter Three concludes by proposing that one way to address this problem is to build a new conceptual construct of territorial privacy which can sustain effective privacy protection and work along-side, rather than be consumed by, informational privacy.

2. Conceptual Foundations of Privacy

It has become standard to start theoretical discussions about privacy by mentioning the conceptual chaos surrounding the term itself.[22] This supposed chaos does not actually appear as bad as it once was. Yes, at the heart of the debate is privacy's protean capacity to be so many things to so many people.[23] As a result, privacy is a complex and multi-faceted concept that resists simple analysis. However, across the broad, often overlapping, range of privacy conceptions produced, three main types or themes can be identified, broadly grouped as non-intrusion, inaccessibility, and control over personal information, each of which are briefly described in this section. These three themes basically map onto the core dimensions used in law; personal/bodily, territorial and informational privacy. Each has merit in articulating core characteristics of privacy. Each, however, has limitations to serve as a unified conceptual basis for sustaining privacy protection. Critiques of these theories of privacy tend to share a common view, seeing them as being too narrow or too broad, or

---

[1993] 3 SCR 519 (the right to security of the person included a privacy right with respect to decisions concerning their own bodies).

[22] A significant portion of the extensive academic literature in this area is dedicated to the preliminary task of defining what privacy is. For comprehensive reviews of the theoretical conceptions of privacy, see for example, Solove, *Understanding Privacy*, *supra* note 17; Ferdinand Schoeman, *Philosophical Dimensions of Privacy*, ed, (Cambridge: Cambridge University Press, 1984); Judith Wagner DeCew, *In Pursuit of Privacy: Law Ethics and the Rise of Technology* (Ithaca, NY: Cornell University Press, 1997).

[23] Binnie J. in *Tessling*, *supra* note 8 at para. 25, privacy is "a protean concept" meaning that it tends to be highly variable and change.

paradoxically, both.[24] For Lisa Austin, the limitations of privacy theory to provide an entirely adequate account of privacy is particularly acute when emerging technology "creates privacy issues that appear to fall outside the bounds of traditional analysis…we do need to sharpen and deepen our understanding of traditional concerns regarding privacy in order to respond to these new situations."[25] Helen Nissenbaum's contextual integrity framework,[26] and Daniel Solove's pragmatic theory of privacy,[27] seek to address the theoretical deficits in privacy discourse, and ultimately do provide useful frameworks for assessing privacy harms. However, both Nissenbaum and Solove mainly address informational privacy rather than the spatial dimensions of privacy. This dissertation suggests that the sharpening of privacy understandings is to reassert the importance and significance of spatial privacy. Ultimately, the problem is not so much determining exactly 'what privacy is' as how do we sustain privacy protection against the proliferation of ubiquitous surveillance in our everyday lived embodied spaces.

2.1 Non-intrusion

The first group of definitions takes non-intrusion as its starting point, a conceptualization highly influenced by Samuel Warren and Louis Brandeis' seminal article, "The Right to Privacy."[28] Namely, and most particularly, the Warren and Brandeis non-intrusion theory of privacy largely informs constitutional search doctrine protecting physical spaces such as the home. Private life, in their view, concerns emotions, sensory experiences, feelings, thoughts and dealings, and includes personal relationships, writings and statements.[29] To protect these interests, Warren and

---

[24] For a comprehensive analysis and critique of the array of privacy theories, see for example, Solove, *Understanding Privacy*, *supra* note 17.

[25] Lisa Austin, "The Privacy Interests at Stake in Public Activities" (Spring 2006) *Innovate Magazine* 18, online: Centre for Innovation Law and Policy <http://www.law.utoronto.ca/documents/publications/Innovate06.pdf>.

[26] Nissenbaum, *Privacy in Context*, *supra* note 13.

[27] Solove, *Understanding Privacy*, *supra* note 17.

[28] Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harv L Rev 193.

[29] *Ibid* at 195.

Brandeis conceived of privacy as the "right to be left alone"[30] or being free from intrusion. In other words, limiting the ability of others to intrude on any of the interests they had articulated as being private, presumably within the purely private domain, and broadcast them to the world.

The 'right to be left alone' suggests a state of solitude and seclusion. Warren and Brandeis actually use the term "solitude" in describing privacy and the necessity for individuals to sometimes "retreat from the world."[31] Alan Westin described this as a need for a "back stage area" because no individual can "play indefinitely, without relief, the variety of roles that life demands" while interacting in public.[32] Charles Fried asserts that private space was necessary as "a context for respect, love, friendship, and trust" which is why "a threat to privacy seems to threaten our very integrity as persons"[33] and thus tying the spatial concept of privacy to personhood. Similarly, Neil Richards argues that spatial privacy is necessary for thought development,[34] and Julie Cohen claims that private space affords "the freedom to dictate the circumstances – the when, where, how, and how often – of one's own intellectual consumption, unobserved and unobstructed by others."[35]

Ultimately, the 'right to let alone' assumes a division of the world into private and public spheres, claiming immunity from intrusion within a special zone of action or one's private affairs. This carries with it a set of difficulties, among them, "it is no easy matter to define a zone of non-interference, as J.S. Mill and innumerable other liberals have discovered."[36] In defending freedoms of the individual against social and political

---

30 *Ibid* at 195, but note the phrase is actually borrowed from Thomas M Cooley, *A Treatise on the Law of Torts or the Wrongs which Arise Independent of Contract*, 2nd ed (Chicago: Callaghan & Co, 1888) at 29.

31 *Ibid* at 196.

32 Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1970) at 35-36.

33 Charles Fried, "Privacy" (1968) 77 Yale LJ 475 at 477.

34 Neil Richards, "Intellectual Privacy" (2008) 87 Texas Law Rev 387 at 412-416.

35 Julie Cohen, "DRM and Privacy" (2003) 18 Berkeley Tech LJ 575 at 579.

36 Arthur Schafer, "Privacy: A Philosophical Overview" in D Gibson, ed, *Aspects of Privacy Law: Essays in Honor of John Sharpe* (Toronto, ON: Butterworths, 1980) 1 at 12. For discussions on the history and nature of the public-private distinction, see for example, Morton Horowitz, "The History of the Public-Private Distinction" (1982) 130:6 Univ. Penn. L. Rev. 1423; Jeff Weintraub, "The Theory and Politics of the Private/Public Distinction" in Jeff Weintraub & Krishan Kumar, eds, *Public and Private Thought and Practice: Perspectives on a Grand Dichotomy* (Chicago: Univ. of Chicago Press, 1997); Hannah Arendt, *The*

control, Mill argued that "there is a limit to the legitimate interference of collective opinion with individual independence; and to find that limit, and maintain against encroachment, is as indispensable to a good condition of human affairs as protection against political despotism."[37] This suggests a public-private distinction which ensures that the legitimacy of interference with individual action is continually under scrutiny. This, in turn, implies that individuals and individual actions are of considerable importance in at least one sphere, the private, and further, it assumes maintaining the boundary between the two spheres is a good thing.[38]

The assumption underlying this position is that a clear line can be drawn between what should remain private and what is in the public domain. It is not simply a question of certain matters changing from being clearly public to private or clearly private to public. Rather, "[p]articular matters have long remained private but in different ways; they have been understood as private but because of different attributes; or they have been regarded as private for some people or groups but not for others. In other words, to say simply that something is public or private is to make a rather general claim; what it means for something to be private is the central question."[39] Moreover, privacy in its traditional context, a simple public-private

---

Human Condition (Chicago: Univ. of Chicago Press, 1958); Jurgen Habermas, *The Structural Transformation of the Public Sphere* (Cambridge, MA: MIT Press, 1989); Milton Konvitz, "Privacy and the Law: A Philosophical Prelude" (1966) 31 Law & Contemporary Problems 272; Catharine MacKinnon, *Feminism Unmodified* (Cambridge, MA: Harvard University Press, 1987; Gavison, "Feminism and the Private-Public Distinction" *supra* note 10; Mimi Sheller and John Urry, "Mobile Transformations of 'Public' and the 'Private' Life" (2003) 20:3 Theory, Culture, and Society 107.

37 John Stuart Mill, *On Liberty and Other Essays*, John Gray, ed (Oxford, UK: Oxford University Press, 1991) at 83.

38 Warren and Brandeis briefly defined private versus public in the spatial sense, but only through a metaphor and without actual mention of the world 'public.' Specifically, they declared, "[t]he common law has always recognized a man's house as his castle, impregnable, often, even to its own officers engaged in the execution of its commands. Shall the courts thus close the front entrance to constituted authority, and open wide the back to idle or prurient curiosity?" "The Right to Privacy" *supra* note 28 at 220. By referring to a "man's house as his castle" they appear to draw a line between what a man does within his own home and what he does outside of that particular zone of privacy. This analysis has persisted and informs Section 8 privacy jurisprudence, largely reflecting the assumption that "so long as the public does not interfere with [private life], autonomous individuals interact freely and equally": MacKinnon, *Feminism Unmodified, supra* note 36 at 99.

39 Solove, *Understanding Privacy*, *supra* note 17 at 50. See also, for example, Gavison, "Feminism and the Public/Private Distinction", *supra* note 10 at 6, noting that, like privacy, the terms 'private' and 'public' are used in different senses.

distinction, is far less relevant today as the boundary between them becomes increasingly blurred when technology spreads across the fabric of every part of our lives. Adam Greenfield has gone so far as to declare that "the only bastion for privacy in this technological future may be in the home because in public space, the battle is already over and the forces of privacy have lost."[40] Helen Nissenbaum argues, for precisely this reason, a theory of privacy in public has never fully developed because until the advent of modern technology it has never really been an issue.[41]

Yet, implicit in the notion of intrusion rooted in Warren and Brandeis' right to be let alone is that actions occurring in public places cannot be private, putting the primary emphasis on physical areas in defining the scope of privacy. This 'no privacy in public' is reflected in the plain view/open fields doctrine[42] and in cases where the courts have relied on the 'public exposure'[43] and 'abandonment'[44] principles to find that a person had no, or a diminished, expectation of privacy.

Underlying these principles is the idea that people effectively assume the risk of scrutiny when they leave their private places. Public privacy does seem counter-intuitive if you think of public-private in the traditional sense – what is public, by definition cannot be private. However, the distinction between public and private cannot be so sharply drawn and privacy is not an absolute. While we may surrender a certain level of privacy when we leave a place of physical solitude into public view, it

---

40 Adam Greenfield, "Everyware: Some Social and Ethical Implications of Ubiquitous Computing" (Keynote address, delivered at Pervasive 2007, the 5th International Conference on Pervasive Computing, Toronto, Canada, 14 May 2007).

41 Nissenbaum, *supra* note 13.

42 In the context of section 8 of the *Charter*, a person has no reasonable expectation of privacy in respect of things that are in plain view and thus there is no 'search' of evidence that is observed by any of the senses in plain view: see for example, *R* v *Law* [2002] 1 SCR 227 (safe in an open field); *R* v *Mellenthin* [1992] 3 SCR 615 (search associated with roadside stops of vehicles); in both *R* v *Kokesch* [1990] 3 SCR 3 and *R* v *Chetwynd* (1996) 161 NSR (2d) 391 (SC), the court found police observations made from backyards did not qualify under the open fields doctrine, but both courts stated that there would not have been searches within the meaning of section 8 if the officers had observed the activities from a "public" area, such as a roadway. As a general principle, aerial observations made from a height expected to be used by the "flying public" will qualify under the open field doctrine and will not constitute a search within the meaning of section 8: *R* v *Cook* (1999) 245 AR 8 (QB).

43 See for example, *Tessling*, *supra* note 8 (heat emanations from the house).

44 See for example, *Patrick*, *supra* note 21 (garbage left at the property line of the house).

does not follow that we forfeit all legitimate expectations of privacy. Traditionally, we have defined privacy in terms of physical barriers such as walls, fences and curtains, but this is too narrow because it ignores the plurality of realms and interactions of our everyday lives in which we carry out private activities in public and does not take into account the desire to protect anonymity. Alan Westin and Ruth Gavison, for example, have recognized that privacy could be invaded in public.[45] While people do not expect solitude and total freedom from observation when they go to the store or other public places, "they do not expect to be under secret surveillance, especially in those times and places for which social custom has set some norms of privacy, even in 'public' situations."[46] Both Westin and Gavison recognize the ability to move around in public anonymously as an important aspect of privacy.[47]

For Nissenbaum, privacy scholars have attempted to contextualize the enhanced practices of surveillance and information aggregation within existing legal and philosophical theories of privacy, struggling with how to build a theory of 'privacy in public.' Yet, many theories of privacy fall short of properly addressing the problem of privacy in public, either dismissing it or ignoring it altogether.[48] Nissenbaum cites conceptual,[49] normative[50] and empirical factors[51] as contributing to the general

---

[45] Westin, *supra* note 32; Ruth Gavison, "Privacy and the Limits of Law" (1980) 89 Yale LJ 412. Others have defined privacy in ways that are broad enough to allow for recognition of a right to privacy in public. See for example, Richard Parker, "A Definition of Privacy" (1974) 27 Rutgers L Rev 275-, 280-281 (defining privacy as control over who senses us); Ernest Van Den Haag, "On Privacy", in Roland Pennock & John Chapman, eds, *Nomos XIII: Privacy* (New York: Atherton Press, 1971) 149-168 (defining privacy as the exclusive access of a person to a realm of his own, which includes the right to exclude others from watching, utilizing or invading his private realm); see also inaccessibility theories, *infra* Section 2.2.

[46] Westin, *supra* note 32 at 112.

[47] For a review and analysis of anonymity and the law in Canada, see Carole Lucock & Katie Black, "Anonymity and the Law in Canada" in Kerr, Steeves & Lucock, *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked* Society (Toronto, ON: Oxford University Press, 2009) *supra* at 465.

[48] Nissenbaum, *supra* note 13.

[49] *Ibid* at 25. Conceptually, the idea that privacy might somehow be violated in public space is often considered paradoxical. For many theorists, the value of privacy applies to an individual's private sphere alone. This thinking follows the lines of a private-public dichotomy, marking distinct realms of personal information on the one hand, and the non-sensitive on the other. In this sense, one's right to privacy is situated as a method of keeping government out of the private lives of individuals to protect intimate or sensitive information against government intrusion. Under this conceptualization, the government has no right to the sensitive, personal, information of what goes on in private space, but would, for example, have the right to the non-sensitive, or public, information of what tollbooth your car passes through. Driving

disregard of privacy in public. A common fear among privacy scholars, in Nissenbaum's view, is that "an ever-growing array of technology-based systems and practices have radically altered the flows of personal information" in a manner that conflicts with the public-private dichotomy which is "commonly supported in academic work and supported in law and policy."[52] Privacy laws have not kept up with the issues that have developed in the wake of advanced technologies and the problem of privacy in public is a key casualty of this oversight.[53] The "mechanisms to deal with conflicts involving privacy in public have generally not taken up the hard questions about surveillance in non-intimate realms to determine when such surveillance is morally acceptable and when not."[54] Many new socio-technical and sensing technologies used for public surveillance, fall into grey areas, or outside current privacy principle, so there is no clear understanding of privacy in these situations. In response, Nissenbaum develops her framework for "privacy as contextual integrity" which views privacy as the appropriate flow of information rather than as a static act of sharing.[55]

---

your car is considered a public act and collecting license plate numbers, displayed in full public view, would not consist of an intrusion into sensitive information.

50 *Ibid* at 72. Normative arguments for the preservation of privacy recognize that privacy, as an important value and interest, must be balanced against other, competing interests. For example, many people are willing to relinquish privacy by allowing their luggage to be searched in airports because safety and security are judged, on balance, more important in such situations. Moreover, since a lot of personal information collected in situations of public surveillance is considered innocuous it is easy for other, competing interests to outweigh the need to keep such information private. See also, David Lyon, *Surveillance Society: Monitoring Everyday Life* (Buckingham, UK: Open University Press, 2001).

51 *Ibid* at 16. Why privacy in public is overlooked also recognizes that the empirical status of privacy in public has failed to garner sufficient attention by privacy theorists. Prior to the recent advances in technology, the problem of privacy in public was not experienced in one's everyday life to the extent it is today. In the past, most people reasonably assumed that their daily and routine movements and activities were neither under surveillance. Individuals carrying out their activities in public would likely be observed, even noted, but there was no general or systematic threat to privacy in public. In sum, the problem of privacy in public was simply not compelling enough to garner significant attention by privacy theorists.

52 *Ibid* at 125.

53 Similar arguments have been made by others. See for example, Elizabeth Paton-Simpson, "Privacy and the reasonable paranoid: The protection of privacy in public spaces" (2000) 50:3 UTLJ 305-346; Krista Boa, "Privacy Outside the Castle: Surveillance Technologies and Reasonable Expectations of Privacy in Canadian Judicial Reasoning" (2007) 4:4 Surveillance & Society 329-345.

54 Helen Nissenbaum, "Protecting Privacy in an Information Age: the Problem with Privacy in Public" (1998) 17 Law & Phil 559 at 579.

55 Nissenbaum, *Privacy in Context*, *supra* note 13.

Privacy as contextual integrity is not a full theory of privacy, but instead a benchmark theory, a conceptual framework that links the protection of personal information to the norms of specific contexts. Rejecting the historical sharp public-private dichotomy, contextual integrity recognizes that all of the activities people engage in take place in a "plurality of distinct realms" in which each realm, or context involves, "indeed may be defined by, a distinct set of norms, which governs its various aspects such as roles, expectations, actions, and practices."[56] Contextual integrity emphasizes that there is no aspect of human life that is "not governed by [context-specific] norms of information flow" whether cultural, ethical or moral norms.[57] Within each of these contexts, norms exist which both shape and limit our roles, behaviours and expectations. In other words, all arenas of life are governed by norms of information flows. Norms of information flow govern what type and how much personal information is relevant and appropriate to be shared with others. Norms of appropriateness "circumscribe the type or nature of the information about various individuals that, within a given context, is allowable, expected, or even demanded to be revealed"[58] and similarly, norms of flow, or distribution, govern how personal information is shared within any given context. Contextual integrity is maintained when both the norms of appropriateness and the norms of flow are respected. Conversely, if either norm is violated in a particular context, the contextual integrity of the flow of information is violated.[59]

Rather than aspiring to universal prescriptions for privacy in public, contextual integrity works from within the normative bounds of a particular context. It tackles head on – and in fact this is the strength of Nissenbaum's model – the one-dimensional private-public distinction by encouraging a recontextualization model where

---

[56] *Ibid* at 137.

[57] *Ibid*.

[58] *Ibid* at 138.

[59] Lisa Austin argues that Nissenbaum's norms of appropriateness are akin to social norms at the heart of the reasonable expectation of privacy test. Austin concludes that the ambiguities in both Nissenbaum's contextual integrity model and the reasonable expectation of privacy standard ultimately undermine privacy because neither have a clear independent normative justification for privacy: "Privacy and the Question of Technology" (2003) 22:2 Law & Phil 119.

information ought to be distributed and protected according to norms governing distinct social contexts. Instead of looking at the tension between the public and the private as a divide, or a dichotomy, Nissenbaum's privacy model speaks to the shifting boundaries between the two as fluid and permeable, which in turn, speaks to the hybridization of virtual and physical worlds.[60]

While Nissenbaum's framework is grounded in the protection of personal information, it is not inconsistent with the spatial dimension of privacy. For example, location still matters simply because certain things, behaviours or physical presence are considered either appropriate or inappropriate to that place, or setting. This is not to suggest that the protection of spatial privacy should be linked exclusively to location or place. Rather, when other people breach a context-specific norm, they take away our control over the realms in which we engage in private affairs or activities. In other words, when someone takes control over your personal information, they take away control over your private space, however it is defined. Viewed in a different way, one reason for protecting the spatial dimension of the privacy interest is to facilitate control over personal information. Ultimately, although the focus of Nissenbaum's contextual integrity model is on informational privacy, although Nissenbaum's contextual features of our everyday lives do factor into the new conceptual construct of territorial privacy proposed in later chapters.

For Julie Cohen, public surveillance threatens the conditions of both "visual and informational exposure."[61] In response, Cohen proposes a characterization of privacy as an "interest in avoiding or selectively limiting exposure" that is meant to extend to people in public spaces.[62] Similarly, Lisa Austin views one part of privacy as "respite from public gaze" as a means to protect aspects of individuality made vulnerable by visual and informational exposure.[63] When under surveillance, "the wrong is that

---

60 See Chapter One, "Hybridization" at p.39.

61 Julie Cohen, "Privacy, Visibility, Transparency and Exposure" 75 Univ Chicago L Rev 181-201, at 201.

62 *Ibid* at 181.

63 Austin, "Privacy Interests", *supra* note 25 at 20.

something that is private has been exposed to view."[64] This explains why we might have a privacy interest in public, but it is "the practices of public surveillance that increasingly disturb us and that appear difficult to articulate within privacy's traditional focus on private spheres."[65]

There is a reading of the Warren and Brandeis definition of privacy as the right to be let alone that supports the position of privacy in public. The Warren and Brandeis articulation of privacy has been interpreted as placing individual rights in a social context and giving individuals the right to determine the boundaries of interaction:

> [T]here is a plain and simple construal of 'right to privacy' for which 'the right to be alone' is a good paraphrase. All societies enforce rules and conventions that carve out a boundary between matters that are socially regulated [i.e. public] and those left to individual discretion and control [i.e. private]. The boundary is multi-dimensional….The right of privacy in a particular society is fixed by the ensemble of the protections against social regulation and control that are established by the society's current rules and conventions….The right to privacy in the critical sense is the right to privacy that morally ought to be accepted and enforced in a particular society.[66]

Interpreted in this way, the right to be let alone provides freedom from intrusion and also freedom of action. The right to be let alone is not just about the right to be in a private place or to have solitude or intimacy, but also about establishing limits to how much one must give up when one ventures into public space. As elaborated on in Chapter Five, this interpretation is important because it recognizes the ability to be 'public' sometimes and the extent to which privacy expectations arise in social interactions. This embraces the concept of privacy as important for developing the self and identity through relationships. Moreover, whether it is freedom to walk down the street, to drive to the store or to sit on a coffee shop patio without being under surveillance and unrecorded, the privacy concern is the same; to be able to carry out and move in our daily activities, to perform in the public sphere, without having our limits crossed or being unable to retreat.

---

[64] *Ibid*.

[65] *Ibid*.

[66] Richard Arneson, "Egalitarian Justice Versus The Right to Privacy?" (2000) 17 Soc. Phi & Policy 91 at 92.

2.2 Inaccessibility

The second of the three main groupings of privacy conceptions is characterized as 'inaccessibility to self' as the underlying basis for protecting privacy. Privacy as inaccessibility is an important part of the umbrella concept of privacy to the extent that it describes many of the central concerns of spatial privacy. Building on the core ideas of Ruth Gavison[67] and Anita Allen,[68] others, such as Nicola Foreham[69] and Christena Nippert-Eng,[70] offer nuanced and analytically useful variations of inaccessibility privacy.

Gavison defines privacy as "a limitation of others' access to the individual."[71] Privacy as limited accessibility refers to "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." [72] In a state of perfect privacy, which Ruth Gavison acknowledges is impossible and generally undesirable, a person would be completely inaccessible to others based on "three independent and irreducible elements: secrecy, anonymity and solitude."[73] Secrecy, because no one will have any information about you; anonymity, because no attention will be paid to you; and solitude, because no one will have physical access to you. Physical access means 'physical proximity' in that someone is "close enough to touch or *observe*" you through normal use of the senses.[74]

---

67 Gavison, *supra* note 45.

68 Allen, *Uneasy Access, supra* note 10.

69 Nicole Moreham, "Privacy in the Common Law: A Doctrinal and Theoretical Analysis" (2005) 121 LQR 628.

70 Christena Nippert-Eng, "Privacy in the United States: Some Implications for Design" (2007) 1:2 International Journal of Design 1-14 and *Islands Of Privacy*, (Chicago, ILL: Chicago University Press, 2010).

71 Gavison, *supra* note 45 at 428. See also Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation* (New York: Random House, 1989) who sees the foundation of the right to privacy as the desire to control identity, which is "the sense of what we identify ourselves as, through and with." (at 20) For Bok, "privacy is "the condition of being protected from unwanted access by others – either physical access, personal information, or attention." (at 10); Wagner, *In Pursuit of Privacy*, *supra* note 22 at 76-77, describing "accessibility privacy" as more than merely information or knowledge but more centrally about observation and physical proximity.

72 Gavison, *Ibid* at 423.

73 *Ibid* at 433. Similarly, under Alan Westin's typology, anonymity, solitude and reserve are identified as states of privacy. Reserve is one of the functions privacy performs which refers to the creation of a psychological barrier against intrusion. Reserve means that you wish to limit accessibility to yourself or communication about yourself to others: *Privacy and Freedom*, *supra* note 32 at 32-39.

74 *Ibid.*

Gavison states, in what seems a carefully worded footnote, that the adjective 'perfect' in 'perfect privacy' was used only as a "methodological starting point."[75] She makes clear that she was attempting to devise a "neutral" and "descriptive" concept of privacy rather than engineering a value proposition that would potentially lead to when we might claim a legal right to protection for privacy.[76] For this reason, Gavison was of the view that incorporating issues of 'control' or of choice would not give rise to a value-neutral notion of privacy.[77] Moreover, once one begins to ascertain when legal remedies ought to be available, one is no longer dealing with the 'neutral' account of privacy as a concept. Thus, Gavison concluded that the "value of privacy can only be determined at the conclusion of discussion about what privacy is, and when – and why – losses of privacy are undesirable."[78]

Anita Allen developed her own "restricted access" definition of privacy as "a condition of inaccessibility of the person, his or her mental states, or information about the person to the senses or surveillance devices of others."[79] For Allen, "[t]o say that a person possesses or enjoys privacy is to say that, in some respect and to some extent, the person (or the person's mental state, or information about the person) is beyond the range of others' five senses and any devices that can enhance, reveal, trace or record human conduct, thought, belief, or emotion."[80] Thus, a "person can be inaccessible in at least three senses: physically, dispositionally, and informationally."[81] The loss of privacy occurs "when a person (or the person's mental states or information about the person) is to some degree or in some respect made more accessible to others."[82] The types of access that one may have can be either direct or

---

[75] *Ibid*.

[76] *Ibid* at 424-425.

[77] *Ibid* at 426-428.

[78] *Ibid* at 425. But it is for this very reason, according to Daniel Solove, that privacy as limited access fails because it does not make clear what types of access implicate privacy and neglects individuals' ability to choose to reveal aspects of themselves to others: Solove, *Understanding Privacy*, *supra* note 17 at 20-21.

[79] Allen, *Uneasy Access*, *supra* note 10 at 15.

[80] *Ibid.*

[81] *Ibid* at 16.

[82] *Ibid* at 17.

indirect. Direct access is possible through one of the five senses unaided. Indirect access is possible through a surveillance device capable of contemporaneous sensory enhancement.[83]

Others have offered valuable variations on the inaccessibility theme. Nicole Moreham, for example, claims privacy is best defined as the state of "desired inaccess."[84] A person would be in a state of privacy only if she is heard, seen, touched or known about if, and to the extent that, she wants to be. Something is private if a person has a desire to be free from outside access in relation to a place, event, activity or information about you. Desire, therefore, acts as an important "limiting or controlling factor" but also introduces a highly individual and subjective factor.[85] In this way, Moreham moves away from Gavison's concept of privacy as a state or condition to framing it as a claim, a shift from a descriptive to a normative conception of privacy.

For Christena Nippert-Eng, privacy "largely centers on the degree to which an individual believes she or he has control over accessibility of things that are private. This might be some aspect of self (including one's body), a thought, a behaviour, relationship, piece of information, chunk of time, a certain space, or an object."[86] In other words, privacy extends from the body to time, space, social relationship and information. Nippert-Eng further suggests that privacy is understood as the condition of pure inaccessibility and publicity as the condition of pure accessibility, while a spectrum of understanding lies between them.[87] Real-world experiences and real-world things fall somewhere in between these public-private endpoints...[s]omething may be relatively more private or relatively more public, but it is never purely

---

[83] *Ibid*.

[84] Moreham, *supra* note 69 at 636. See also, Jean Cohen, *Regulating Intimacy: A New Legal Paradigm*, (Princeton: Princeton University Press, 2002) at 57, describing that an essential aspect of privacy is the ability to, in an authentic manner, determine for oneself certain ways of acting and to present oneself to others in ways one is comfortable being seen and assessed…this ability in terms of "[c]ontrol over one's identity, over access to oneself, over which aspects of oneself one will present at which time and to whom, along with the ability to press or to waive territorial claims that is crucial and empowering."

[85] Moreham*, ibid* at 643-644, acknowledges the need for an objective check if her definition is to be employed in the legal context.

[86] Nippert-Eng, "Privacy in the United States" *supra* note 70 at 1.

[87] *Ibid* at 3.

either."[88] Thus, when we think about privacy, what we really think about is "a condition of *relative* inaccessibility. Any point on the scale has both a degree of privateness and a degree of publicness associated with it, that is, an emphasis on one may far outweigh but never completely displace the simultaneous presence of the other."[89] The concepts 'private' and 'public' or 'privacy' and 'publicity' are "concepts that are coupled and related to each other in the same way as islands and oceans, land and water. This is key to understanding how our culture conceptualizes privacy."[90] Unfortunately, as discussed later in this chapter, courts have had difficulty giving legal protection where there has been spatial access, but no physical intrusion, thus have tended to interpret spatial access in terms of informational access.

Although social interaction theories do not fall within conventional theories of privacy, Irwin Altman regarded one of privacy's major functions as serving the individual's self-identity by creating personal boundaries.[91] He defined privacy as "a selective control of access to the self or to one's group."[92] Rather than static, Altman regards privacy as a dialectic and dynamic boundary regulation process where people optimize their accessibility along a spectrum of "openness" and "closedness" depending on context. Privacy becomes then "the negotiated line between the two."[93] In effect, Altman is creating pockets of accessibility as a way in which we try to achieve some privacy, not unlike Moreham's 'desired inaccess' conception of privacy and

---

88 Nippert-Eng, *Islands Of Privacy*, *supra* note 70 at 5.

89 *Ibid* at 5.

90 *Ibid* at 4.

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

See also, Alan Westin, *supra* note 32 at 7, privacy, when viewed in terms of the relation of the individual to social participation, is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude of small-group intimacy or, when among larger groups, in a condition of anonymity or reserve. The individual's desire for privacy is never absolute, since participation in society is an equally powerful desire. Thus each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives.

92 Altman*, ibid* at 18. Conceptualizing privacy in this way not only promotes the development of intimate relationships, but also one's evolving sense of identity (at 77-79).

93 Steeves, "Reclaiming the Social Value of Privacy," *supra* note 17 at 202.

Nippert-Eng's 'relative inaccessibility.' For Altman, Moreham and Nippert-Eng, making some parts of ourselves accessible to some people in some times and places actually helps us get away with denying them access to other parts or other places and times. It is within this context, for Altman, that the negotiating process of defining and defending boundaries or privacy is understood. In Chapter Five, boundary management is discussed further as it forms one of the key defining features of the alternative conceptual construct of territorial privacy being proposed in this dissertation.

2.3 Control Over Personal Information

Privacy as control over information is "the claim by individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others."[94] Understanding privacy as control over personal information is at the core of consent-based data protection laws, which function to empower individuals to control access to and use of their personal information.[95]

---

[94] Westin, *Privacy and Freedom*, *supra* note 32 at 7. The dominant definitions of privacy as control over personal information are well documented. See for example, Solove, *Understanding Privacy, supra* note 17; Eloise Gratton, *Understanding Personal Information: Managing Privacy Risks*, (Toronto, ON: LexisNexis, 2013); Mark Andrejevic, "Control Over Personal Information in the Database Era" (2009) 6:3 Surveillance & Society 322—326.

Variations, or sub-sets, of the information-control conception of privacy include, for example, Richard S Murphy, "Property Rights in Personal Information: An Economic Defense of Privacy" (1996) 84 Geo Law Journal 2381 and Vera Bergelson, "It's Personal But is it Mine? Toward Property Rights in Personal Information" (2003) 37 UC Davis L Rev 379, (personal informational as property); Charles Sykes, *The End of Privacy* (New York: St. Martin's Press, 1999)(privacy-as-contract); Teresa Scassa, "Information Privacy in Public Space: Location Data Protection and the Reasonable Expectation of Privacy" (2010) 7 CJLT 199-220 (location information privacy); and Michel Drapeau and Marc Aurele Racicot, *Protection of Privacy in the Private and Health Care Sectors*, (Toronto, ON: Carswell, 2012) (health information privacy).

[95] Most contemporary data protection laws have their roots in the Organization for Economic Cooperation and Development's 'fair information principles.' OECD Directorate for Science, Technology and Industry, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (1980), online: OECD <http://www.oecd.org/sti/>. These principles focus on norms relating to notice, consent, access, and security safeguards. Informed consent is a central principle in most legislative regimes. In Canada, see *Personal Information Protection and Electronics Document Act,* SC 2000 c 5 [*PIPEDA*]; *Personal Information Protection Act*, SBC 2003 c 63; and *Personal Information Protection Act*, SA 2003 c P-6.5.

Data protection laws have been considered in the context of consumer privacy and RFIDs, see for example, Teresa Scassa et al, "Consumer Privacy and Radio Frequency Identification Technology" (2005-2006) 37 Univ. Ottawa LR, 215-248. According to the Canadian Privacy Commissioner, "[i]f the chip has had the

Outside of data protection laws, a conception of privacy as control over personal information excludes what may be legitimately claimed under spatial privacy. As Daniel Solove points out, while "many forms of intrusion are motivated by a desire to gather information or result in the revelation of information, intrusion can cause harm even if no information is involved." [96] Defining privacy as informational control does not get at the core of the objection to intrusions into private places or our everyday lived spaces. In the classic peeping Tom example, whether or not information is obtained about the watched person, the spatial privacy interest is nonetheless engaged. An informational control based approach does not necessarily capture what will often be the primary objection and harm, the secretive invasion. As Raymond Wacks explains: "[w]hat is essentially in issue in cases of intrusion is the frustration of the legitimate expectations of the individual that he should not be seen or heard in circumstances where he has not consented to or is unaware of such surveillance. The quality of the information thereby obtained, though it will often be of an intimate nature, is not the major objection."[97]

2.4 Pragmatism

Much like Nissenbaum's motivation for developing a new privacy framework, for Daniel Solove, "privacy is a concept in disarray" and thus seeks to set out a new approach.[98] While individuals seem to know instinctively when they have suffered an

---

personal information of the individual written to it, then it is a repository of personal information. If the tag is unique, and can be associated with an individual, it becomes a unique identifier or proxy for that individual; and information about possessions or purchases, which can be manipulated or processed to form a profile, is personal information, whether gathered through multiple visits to a facility or organization, or through access to the data base of RFID purchase information." Office of the Privacy Commissioner of Canada, "RFID Technology" (23 February 2006), online: Office of the Privacy Commissioner of Canada Fact Sheets <http://www.priv.gc.ca/resource/fs-fi/02_05_d_28_e.asp>; and applied to location-based-services, see for example: Scassa, Information Privacy in Public Space, *supra* note 91, and David Lyon et al, *Location Technologies: Mobility, Surveillance and Privacy*, Queens University: The Surveillance Project (March 2005) online: <http://www.surveillanceproject.org/files/loctech.pdf>.

In the context of section 8 of the *Charter* and informational privacy interests, see Chapter Three 'Informational Privacy Zone' at p 128.

96 *Ibid* at 163. *Ibid.* See also Gavison, *supra* note 45 at 432, "[a]ttention alone will cause a loss of privacy even if no new information becomes known."

97 Raymond Wacks, *Personal Information: Privacy and the Law*, (Oxford, Clarendon Press, 1989) at 248.

98 Solove, *Understanding Privacy*, *supra* note 17 at 1.

invasion of privacy, theorists and courts are considerably less certain about these violations. As a result, courts, in Solove's view, frequently struggle to find a compelling account of privacy's importance and a framework to guide them in balancing privacy against other legally protected interests. They resort then to a singular notion of privacy to evaluate activities that, in fact, have significantly different privacy implications.[99] The result is that some privacy problems that are distinct are conflated while other privacy problems are not recognized at all.

While Solove, like many before him, set out to "reach a definitive conclusion about what 'privacy' is"[100] he realized that "the quest for a singular essence of privacy leads to a dead end."[101] Traditional methods of conceptualizing privacy, which attempt to locate a common set of necessary and sufficient elements that distinguish privacy from other categories, will always come up short.[102] When the core of privacy is defined to narrowly, important privacy problems are ignored,[103] and if the core of privacy is defined too broadly, the conception lacks sufficient precision to be helpful.

Thus, an alternative to traditional methods of conceptualizing privacy is needed to understand privacy in a meaningful way and Solove formulates his "pragmatic" approach to privacy.[104] Abandoning the search for a common denominator or essence of privacy, he offers a pluralistic vision, which views privacy as an "umbrella term that refers to a wide and disparate group of related things."[105] The approach is grounded in philosopher Ludwig Wittgenstein's idea of family resemblances. Wittgenstein employs the term "family resemblances" to explain that certain concepts do not have a central defining characteristic, but rather, they draw from a pool of similar, and at times,

---

99 *Ibid* at 37.

100 *Ibid* at ix.

101 *Ibid*.

102 *Ibid* at 1-2.

103 For example, concepts like the right of "inviolate personality" and "limited access to the self" may justify privacy protections in certain situations, but none grounds every instance.

104 Solove, *Understanding Privacy*, *supra* note 17 at 87.

105 *Ibid* at 45.

overlapping, "family" characteristics.[106] Solove contends that privacy is such a concept, the meaning of which cannot be reduced to any single thing because, in practice, it describes a cluster of related things.[107] In adopting Wittgenstein's method, Solove suggests that we categorize "something as involving 'privacy' when it bears resemblance to other things we classify the same way."[108] This type of reasoning reflects the way we actually talk about privacy, that is, as a family of interrelated yet distinct things.[109]

There is, of course, value in a "framework for understanding privacy in a pluralistic and contextual manner."[110] However, can this be achieved without an "overarching principle" and do we need one?[111] Solove uses law to account for "privacy problems that have achieved a significant degree of social recognition."[112] The law because "it provides concrete evidence of what problems societies have recognized as warranting attention."[113] For Robert Wacks, the protracted searches and efforts for a definition of privacy has "produced a continuing debate that is often sterile" because the material differences on premises, objectives, the value, and the nature of privacy produce definitions that beg more questions than they answer, so that the exercise as a whole is futile because privacy is whatever the courts and legislature say it is.[114] Presumably, Wacks' observation is meant in the same way as Solove's criteria for inclusion involve recognition of legal rights. However, its similarity to the now (in)famous declaration by Humpty Dumpty that when he uses a word "it means just

---

106 Ludwig Wittgenstein, *Philosophical Investigations*, 2nd ed, GEM Anscombe, trans. (Oxford: Basil Blackwell, 1958) at 66-67.

107 Solove, *Understanding Privacy*, *supra* note 17 at 42-46.

108 *Ibid* at 46.

109 *Ibid* at 44-45.

110 *Ibid* at 10.

111 *Ibid* at 105: "My taxonomy's categories are not based on any overarching principle. We do not need overarching principles to understand and recognize problems."

112 *Ibid* at 101.

113 *Ibid* at 102.

114 Robert Wacks, "The Poverty of Privacy" (1980) 96 L Q Rev 73 at 75-77.

what I choose it to mean, neither more nor less"[115] highlights two difficulties with Solove's privacy framework. First, there are privacy harms that do not fit within a family of resemblances, as for example, when the spatial privacy interest is implicated without the informational dimension, it can be separate and distinct. Second, relying on the law to group privacy harms means the taxonomy will continue, largely, to be a model exclusively concerned with informational privacy. Again, much like Nissenbaum's framework, ultimately it does not adequately capture the entire array of privacy interests, specifically those spatial dimensions of privacy that are the subject of this dissertation.

Although one way to look at the privacy implications of ubicomp is to consider whether a more robust conception of informational privacy would address these issues, an approach that limits analysis to the collection, nature and quality of information does not take into account the physical and personal lived spaces which are increasingly left vulnerable by enhanced surveillance enabled by emerging technologies. Further, an informational approach, on its own, serves to constrain a robust discussion of privacy whereas a robust discussion of spatial privacy enhances and potentially broadens the legal protection of the array of privacy interests.

In conclusion to this section on conceptions of privacy, the need to manage one's privacy runs throughout all of these definitions of privacy, namely, the condition of being alone without intrusions, a state of inaccessibility to things, bodies, places, and control over information collection and disclosure. The core conceptual underpinnings of privacy generally map onto the zonal classification of privacy as principally developed under section 8 of the *Charter*. The remainder of this chapter discusses the extent to which these interests are constitutionally protected under Canadian search doctrine. While each zone of privacy is considered, the focus is on the spatial dimension of privacy, generally classified as territorial privacy.

---

[115] Lewis Carrol, *Alice's Adventures in Wonderland and Through the Looking Glass* (London: Puffin Books, 1996) at 87.

3. Section 8 and the 'Zones' of Privacy

For generations, Canadian search and seizure law was organized around common law principles of property. A 'search' was simply a very specific sort of governmental trespass or interference with an individual's right to property.[116] Canadian constitutional protection against unreasonable searches is found under section 8 of the *Charter of Rights and Freedoms* which provides that everyone has the right to be "secure against unreasonable search and seizure."[117] Described as "vague and open" section 8 offers little guidance on what precisely it guarantees, whereas its American counter-part, the Fourth Amendment which is much more specific.[118] Further, the United States had "a history of colonial opposition to certain Crown investigatory practices from which to draw out the nature of the interests protected by that amendment and the kinds of conduct it proscribes," but in Canada, there is no "particular historical, political or philosophical context capable of providing an obvious gloss on the meaning of the guarantee."[119] Notwithstanding, it was the landmark United States Supreme Court decision in *Katz* that Justice Dickson (as he then was) looked to in interpreting the first section 8 case before the Supreme Court of Canada.[120]

Hunter,[121] decided in 1984, stands for two significant propositions. First, and central to this dissertation, Justice Dickson rejected narrow notions of property as the

---

[116] The most famous of these cases is of course *Entick* v *Carrington* (1765) 19 State Tr 1029, in which the court based its decision in favour of the landowner on the right to property, at 1066, "[t]he great end, for which men entered into society, was to secure their property. That right is preserved sacred and incommunicable in all instances, where it has not been taken away or abridged by some public law for the good of the whole." For statutory purposes, a search is an otherwise unauthorized physical entry onto someone's property to look for physical evidence: section 487, *Criminal Code of Canada* RSC 1985 c C-46.

[117] *Charter*, *supra* note 2.

[118] *Hunter* v *Southam* [1984] 2 SCR 145 at 154 [*Hunter*]. The United States Fourth Amendment, *supra* note 2.

[119] *Hunter ibid* at 155.

[120] *Katz*, *supra* note 4. The concept of constitutional privacy in the United States was principally articulated in 1928 in *Olmstead* v *United States* (1928) 277 US 438, in which the United States Supreme Court held that the Fourth Amendment protection applied only to a person's private property. *Katz* reconceptualized the Fourth Amendment by no longer restricting constitutional protection to a person's private property. The *Katz* majority held that one who occupies a public telephone booth may give rise to a reasonable expectation of privacy. The *Katz* decision is discussed in more detail in Chapter Five.

[121] *Hunter*, *supra* note 118 (at issue was the constitutionality of provisions of the *Combines Investigation Act*, that authorized the Director of Investigation and Research of the Combines Investigation Branch to enter

purpose behind section 8, relying on *Katz* for the proposition that the right against unreasonable searches protects "people, not places," such that privacy, rather than property, is central to the guarantee.[122] The intent of saying that privacy protects "people, not places" was to move privacy protection away from its roots in trespass and, in effect, to bring it into the human rights era. What is, or ought to be, sacred and worthy of protection is not the location or ownership of property, but people. With this in mind, privacy in the context of section 8 is meant to relate in some way to the individual human being and not simply to the particular physical places or geographical coordinates in which the individual happens to be.

The second significant proposition from *Hunter* is that the fundamental objective of section 8 is "to protect individuals from unjustified state intrusion upon privacy by ensuring them a "reasonable expectation of privacy."[123] 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 section 8."[124] 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. Determining whether an expectation of privacy is reasonable requires "an assessment…as to whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement."[125] Thus, the reasonable expectation of privacy test defines the scope of constitutionally protected privacy intrusions. To qualify, a privacy expectation must meet both subjective and objective criteria, the individual must have an actual

---

any premises on which the Director believes there may be evidence relevant to matters being inquired into).

122 *Ibid*.

123 *Hunter*, *supra* note 118.

124 *Tessling*, *supra* note 8 at para 18.

125 *Hunter*, *supra* note 118 at 159-160.

expectation of privacy, and that expectation must be one that society recognizes as reasonable.[126] What then is the scope of the reasonable expectation of privacy?

It has become almost conventional to speak of the zones of privacy as personal (or bodily), territorial and informational as an analytical framework for understanding the core dimensions of privacy.[127] These dimensions are meant to go some way towards accounting for the underlying interests that privacy as a concept purports to protect by interpreting "three ways of describing the normativity of privacy."[128] In other words, each of the dimensions lies at the heart of a normative theory of privacy. In Canada, privacy claims as articulated under section 8 jurisprudence may relate to personal, territorial and informational privacy interests.[129] While initially appealing as a conceptual device, the categorization is less effective in today's very different computing environment where traditional dichotomies for space, person and time are easily deconstructed. Moreover, within each category, the privacy interest has been narrowly interpreted by the Supreme Court of Canada and fails to take into account the nature of changing technologies. Each dimension is considered here, but the focus is on the territorial model of spatial privacy.

Bodily/Personal Privacy Zone

Bodily, or personal, privacy refers to an individual's interest in the "sanctity of a person's body."[130] A heightened privacy interest is generally recognized in one's body "because it protects bodily integrity, and in particular the right not to have our bodies touched or explored or disclose objects or matters we wish to conceal."[131] Bodily or personal privacy is engaged when there is an intrusion *into* the body,[132] basically strip

---

126 *Ibid* at 159; *Edwards* [1996] 1 SCR 128 at para 45 [*Edwards*].

127 Rossler, *supra* note 11.

128 *Ibid* at 9.

129 *Dyment*, *supra* note 20; *Tessling*, *supra* note 8; *Patrick*,*supra* note 21.

130 *Dyment*, *supra* note 20 at para 21.

131 *Tessling*, *supra* note 8 at para 21.

132 *R v Pohoretsky*, [1987] 1 SCR 945 at 949, "[a] violation of the sanctity of a person's body is much more serious than that of his office or even his home." See also, *R v Simmons*, [1988] 2 SCR 495; *R v Greffe*, [1990] 1 SCR 755; *R v Stillman*, [1997] 1 SCR 607.

searches, or when bodily substances are taken *from* the body in which information is obtained.[133] Bodily privacy is also spatial; the person is deemed to be surrounded by a space, but unlike physical property, it is not necessarily bounded by tangible barriers. Its realm transcends "the physical and is aimed at protecting the dignity of the human person."[134] Bodily privacy can be said to relate to a sphere of the self; a zone of privateness surrounding the individual, which should not be intruded on without justification by either unwarranted physical contact or by unwarranted observation. This zone of privacy also surrounds personal information and data about an individual.[135] Although Justice LaForest's 'personal space' privacy interest is meant to be concerned with invasions of the body in the moral sense,[136] it has not been effectively tested outside physical intrusions and therefore, on the current construction of personal privacy, new forms of surveillance arising from technology in and around the body, may not engage section 8.[137]

Territorial Privacy Zone

The classification of 'territorial privacy' includes privacy's meaning in the most classical sense, physical privacy, or privacy of private space. The persistent tendency towards the territorial construct is understandable considering property and privacy are inextricably linked to concepts of spatial exclusion. This tendency also reflects the traditional presumption that the "house of everyone is to him as his castle and

---

133 *Dyment*, *supra* note 20 at para 27 "[t]he use of a person's body without his consent to obtain information about him, invades an area of personal privacy essential to the maintenance of his human dignity." See also, *R* v *S.A.B.* [2003] 2 SCR 678 (DNA testing); *R* v *Briggs* (2001) 157 CCC (3d) 38 (OntCA) (databanking).

134 *Dyment*, *ibid* at para 21.

135 *Ibid* at para 22.

136 *Ibid* at para 21.

137 Body scanners in use at many North American airports, however, represent a shift from current biometric technology, facilitating a technologically-mediated strip search without physical intrusion. Olga Mironenko, "Body Scanners Versus Privacy Versus Data Protection" (2011) 27 Computer Law & Security Review 232-244; Andrea Slane, "From Scanning to Sexting: The Scope of Protection of Dignity-Based Privacy in Canadian Child Pornography Law" (2010) 48 Osgood Hall LJ 543. The federal Privacy Commissioner has concluded that airport body scanners comply with federal data protection laws: Office of the Privacy Commissioner of Canada, *Privacy & Aviation Report* (2011), online: <http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_catsa_2011_e.pdf>.

fortress."[138] This formed a critical cornerstone in the development of the American Fourth Amendment jurisprudence upon which section 8 is modeled. The home, "at its most genuine locus… for many people still intuitively represents the heart of privacy."[139] There is consistent support for preserving the sanctity of the home as vital for promoting the values search and seizure seeks to protect.[140] However, the recurring ideal of protecting the traditional home may not be as relevant today when the devices we carry with us are used for private affairs, activities and interaction previously occurring within the home.

Territorial privacy interests have been de-physicalized so that its protection, at least in theory, extends beyond a property analysis to protect people, not places.[141] This envisions that a person's reasonable expectation of privacy is protected not only within certain well-marked traditional enclaves, but everywhere that circumstances might give rise to such an expectation. The territorial privacy interest protects the perimeter of the home,[142] and extending beyond the home, to vehicles,[143] hotel rooms,[144] a public washroom stall,[145] a mental health facility,[146] an apartment[147] and a

---

138 *Semanyne v Gresham* (1604), 77 Eng Rep (KB) 195-196 [*Semanyne*]. See also *Entick*, *supra* note 116; and Jonathon Hafetz, "A Man's Home is His Castle: Reflections on the Home, the Family, and Privacy During the Late Nineteenth and Early Twentieth Centuries" (2002) 18:2 Wm. & Mary J. Women & L 175.

139 Rossler, *The Value of Privacy*, *supra* note 11 at 142.

140 *R* v *Silveira* [1955] 2 SCR 297 (unlawful search because police entered the home without a warrant to preserve evidence); *R* v *Feeney* [1997] 2 SCR (unlawful search because police entered the home to make an arrest without a warrant); *Tessling*, *supra* note 8 at para 22, expressly citing *Semanyne*; and at para 15, citing *Silveira*, "[t]here is no place on earth where persons can have a greater expectation of privacy than within their dwelling-house."

141 *Hunter*, *supra* note 118; *Plant, supra* note 18, confirming that it is not necessary for a person to establish a possessory interest to attract section protections, but going on to adopt an informational analysis holding that there was no reasonable expectation of privacy in computer records of an individual's consumption of electricity at his residence.

142 *R v Grant* [1993] 3 SCR 223; *R v Kokesch* [1990] 3 SCR 3 [*Kokesch*].

143 *R v Belnavis* [1997] 3 SCR 341 [*Belnavis*], but not passengers in the vehicle. The driver/owner of the vehicle has a reduced expectation of privacy: *R v Wise* [1992] 1 SCR 527 [*Wise*].

144 *R* v *Wong* [1990] 3 SCR 36 [*Wong*], but note Justice Lamer's dissent that the hotel room ceased to be a private space when the defendant invited others into the room thus eliminating any reasonable expectation of privacy.

145 *R v O'Flaherty* (1987) 63 Nfld & PEIR 21 (Nfld CA); *R v Silva* (1995) 26 OR 3d 554 (Gen Div), but note *R v LeBeau* (1988) 25 OAC 1 (CA) finding no reasonable expectation of privacy outside the closed toilet cubicle of a public washroom.

146 *R v Smyth* [2006] CarswellOnt 8968 (Ont SCJ).

storage locker.[148] However, on the current territorial assessment, you can still point to areas that are in some way marked off by clear boundaries from the outside world by either tangible barriers or places subject to proprietary control that are sustaining its protection. While trespass is not generally invoked by the courts expressly, the use of these boundaries to delineate when and how a territorial privacy interest is violated is implicit in the result.

Generally, it has been held that there is no protected privacy interest with respect to people or things that are observed in plain view,[149] knowingly exposed[150] or abandoned.[151] The 'no privacy in public' is rooted in the Warren and Brandeis exclusion theory of privacy largely informed by the traditional private-public distinction. If section 8 does not protect 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. 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."[152] Similarly, Daniel Solove criticizes 'no privacy in public' as a "binary understanding of privacy that is both antiquated and inadequate."[153] Technological developments, such as the ubiquity and usage of camera phones and pervasive sensors, threaten privacy in ways not anticipated when the rule first emerged. Thus, since most people reasonably expect to be free from government surveillance on sidewalks, coffee shops, parks and streets; section 8 should not be so strictly interpreted so as to prevent privacy in public altogether. 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

---

147 *R v Pugliese* (1992) 52 OAC 280, but not in common hallways of the apartment building: *R v Laurin* (1997) 98 OAC 50. A visitor to an apartment has no reasonable expectation of privacy: *Edwards*, *supra* note 126.

148 *R v Buhay* [2003] 1 SCR 631.

149 *Law, Mellenthin, Kokesh, Chetwynd, supra* note 42.

150 *Tessling*, *supra* note 8.

151 *Patrick*, *supra* note 21.

152 Reiman, "Driving to the Panopticon" in Rossler, *Privacies*, *supra* note 15.

153 Daniel Solove, *The Future of Reputation: Gossip, Rumour and Privacy on the Internet* (New Haven, CT: Yale University Press, 2007) at 7.

between private and public spatial domains" and instead attend to what constitutes a "reasonable expectation of privacy in a given context."[154] In *Edwards*, the Supreme Court did outline and consider the scope of the reasonable expectation of privacy in relation to places on the basis of "the totality of circumstances," including:

> (i) presence at the time of the search;
> (ii) possession or control of the property or place searched;
> (iii) ownership of the property or place;
> (iv) historical use of the property or item;
> (v) the ability to regulate access, including the right to admit or exclude others from the place;
> (vi) the existence of a subjective expectation of privacy; and
> (vii) the objective reasonableness of the expectation. [155]

Based on these factors, the boyfriend-visitor to an apartment rented by his girlfriend and did not have a reasonable expectation of privacy in relation to that place and therefore the drugs found at that location, belonging to the defendant, were not be excluded from evidence.

Justice La Forest dissented. In his view, the majority's approach would result in a "drastic diminution" of *Charter* protection of privacy by restricting its reach to cases in which "an accused has a personal right to privacy in the sense of some direct control or property."[156] And looking at the factors listed in *Edwards*, it is not a stretch to identify property-inherent principles. He also criticized the majority for its adoption of post-*Katz* jurisprudence from the United States, observing that "[t]he sorry state of the law in the United States is a product of history. It seems unfortunate that this Court has the irresistible urge to repeat it."[157] The result was a model for evaluating privacy interests based on a "series of syllogisms" concluding that "[s]yllogistic reasoning has

---

[154] Justice Gerald LaForest, "Opinion – Video Surveillance (5 April 2002), online: Office of the Privacy Commissioner of Canada Archived News <http://www.priv.gc.ca/media/nr-c/opinion_020410_e.asp>.

[155] *Edwards*, *supra* note 126 at para 30; see also *Plant*, *supra* note 18, in which the court applied these factors to an informational analysis finding no reasonable expectation of privacy in residential hydro records accessible to the public.

[156] *Ibid* at para 59.

[157] *Ibid* at para 66.

its place, no doubt, but that can only be so long as the premises are sound."[158] Reasoning that has reinforced the no privacy in public rule and a property analysis.

Informational Privacy Zone

Informational privacy pertains to a person's right to control personal information.[159] Not every acquisition of information is characterized a search, but rather "it is only where a person's reasonable expectations of privacy are somehow diminished by an investigatory technique that section 8 of the *Charter* comes into play."[160] In order to attract constitutional protection, information must be at "the biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state" and which, if disclosed, would "reveal intimate details" about the "personal lifestyle or private decisions" of the person."[161] In *Plant,* the court concluded that "electricity consumption reveals very little about the personal lifestyle or private decisions of the occupant of the residence" and as such does not give rise to a reasonable expectation of privacy.[162] In *Tessling*, Justice Binnie acknowledged the high expectation of privacy people have in their bodies, homes and work, but beyond these privacy interests "lies the thorny question of how much information about ourselves and activities we are entitled to shield from the curious eyes of the state."[163] The extent to which a person has a reasonable expectation of privacy in personal information depends on the nature and quality of the information.[164] Although there is a reasonable expectation in information

---

158 *Ibid*.

159 *Dyment*, *supra* note 20 at para 22.

160 *R v Evans* [1996] 1 SCR 8 at para 11.

161 *Plant*, *supra* note 18 at para 20.

162 *Ibid*. See also *R v Gomboc*, [2010] 2 SCR 211 [*Gomboc*], involving residential electrical consumption information gathered by the service provider through its power lines and given to police followed *Plant* in finding no reasonable expectation of privacy in the information, but a much more controversial judgment given the DRA technology was able to collect information about what was going on inside the home.

163 *Tessling*, *supra* note 8 at para 23 [emphasis in original]. This case involved police use of infra-red technology to read heat emanations from a home without a warrant. The court adopted an informational analysis finding there was no violation of a reasonable expectation of privacy and thus no search.

164 *Ibid* at 27.

regarding what goes on inside the home,[165] the Supreme Court treated the search in *Tessling* as a search for information about the home and not as a search of the home itself. Thus, since the information revealed by the FLIR was, by itself, meaningless, there was no violation of a reasonable expectation of privacy because the information did not reveal any of the defendant's biographical core.[166] In essence, *Tessling* suggests that the weaker the inference about what is going on in the home, the less the informational privacy interest will be engaged by section 8. Ultimately, as elaborated on in Chapter Five, this narrowing of personal information effectively undermines the protection of spatial privacy interests in the spaces in which we reasonably expect our information will be kept private.

Increasingly, sub-sets of 'informational privacy' are cropping up in the context of ubiquitous computing technologies, most notably, the concept of 'locational privacy.'[167] Locational privacy is the ability to control the access to location information related to an individual.[168] However, whether the nature and quality of the data that may be gathered would be considered 'core biographical information' or sufficiently intimate, personal or private to trigger section 8 is unclear.[169] In other words, location is not inherently private and we do not have our privacy violated every time we share our location with a service or a friend. The likelihood that this type of information, in and of itself, would be considered sufficient to meet the high threshold of what is covered by the reasonable expectation of privacy in personal information is remote at best. This is reinforced by virtually everyone who now routinely asks 'where

---

165 *Ibid* at para 38.

166 *Tessling*, *supra* note 8 at para 36, 62-63.

167 See for example, Mark Monmonier, *Spying With Maps: Surveillance Technologies and the Future of Privacy* (Chicago, IL: University of Chicago Press, 2002); Scassa, "Information Privacy in Public Space" *supra* note 94; Adriana de Souza e Silva & Jordon Firth, "Locational Privacy" (2010) 3:4 Communication, Culture and Critique 503.

168 Alastair R Beresford, "Location Privacy in Pervasive Computing" (2003) 2:1 IEEE Pervasive Computing 46 at 46.

169 *Plant*, *supra* note 18; *Tessling*, *supra* note 8; *Gomboc*, *supra* note 162. For a comprehensive analysis on the evolution of informational privacy in the context of section 8, see Ian Kerr & Jena McGill, "Emanations, Snoop Dogs and Reasonable Expectations of Privacy" (2007) 52:3 Criminal Law Quarterly 392; and David Matheson, "Deeply Personal Information and the Reasonable Expectation of Privacy in *Tessling*" (2008) 50:3 Canadian Journal of Criminology and Criminal Justice 349.

are you' and many freely volunteer this information when interacting via cell phones or using Location Based Services.

Overlapping Privacy Interests

Bodily, territorial and informational privacy interests are generally seen as separate and distinct privacy interests, but it is possible to infringe on more than one of these interests at the same time.[170] The overlap of categories is not insignificant, since how the privacy interest is characterized may dictate the outcome. For example, in *Tessling,* Justice Binnie acknowledged that the territorial privacy interest was implicated when law enforcement measured heat emanations, originating from inside the home, from the external wall. However, he went on to find that the interest engaged was "essentially informational" which led to a very different result than that of the lower court decision which was based on a territorial analysis.[171] Similarly, in *Gomboc*,[172] after an investigation raised suspicions that a grow-op was likely located in Mr. Gomboc's house, police arranged for a digital recording ammeter (DRA) to be installed by electricity provider (Enmax) on its power line to measure and record electricity use. These facts gave rise to a case that "straddles two categories of privacy interests recognized in the jurisprudence," the primary privacy interest is the claim to informational privacy in the electricity records obtained from Enmax and turned over to the police, but also territorial privacy "because the information sought involved an activity taking place with Mr. Gomboc's home."[173] Since there was no "direct search of the home itself" and the home was the focus "of an otherwise non-invasive and unintrusive search" is subsidiary to investigative technique and what information was

---

[170] See for example, *Tessling*, *supra* note 8; *Patrick*, *supra* note 21; *Gomboc*, *supra* note 162; *Jones*, *supra* note 2.

[171] *R v Tessling* (2003), 63 OR (3d) 1 (CA). The Ontario Court of Appeal followed American counterpart *Kyllo*, *supra* note 8, finding the warrantless use of FLIR technology violated the Fourth Amendment protection against search and seizure because it was not a device in general public use and it allowed exploration into the home. Note, however, the U.S. Constitution Fourth Amendment expressly includes 'house' whereas *Charter* section 8 does not.

[172] *Gomboc*, *supra* note 162.

[173] *Ibid* at para 22.

actually disclosed.[174] Thus, a search with a territorial privacy aspect involving the home "should not be allowed to inflate the actual impact of the search to a point where it bears disproportionately on the expectation of privacy analysis."[175] In *Patrick*, Justice Binnie identified two threshold issues. The first was whether Patrick enjoyed a reasonable expectation of territorial privacy because the officers had to reach over his property line to secure the garbage bags. Second, whether he had a reasonable expectation of informational privacy with respect to the contents of his garbage. Fatal to Patrick's claim, wrote Justice Binnie, was its objective reasonableness. With respect to territorial privacy, little significance was attributed to the "relatively peripheral" territorial intrusion that officers made when they reached over Patrick's property line to secure his garbage.[176] Furthermore, objectively speaking, Patrick abandoned his garbage along with any reasonable expectation of privacy in its contents when he placed it at the back of his property for municipal collection. Therefore, after essentially diminishing the territorial privacy interest, while Patrick did have a subjective reasonable expectation of privacy in the contents of his garbage, he risked that it would be disturbed by the public once abandoned and as a result the police could disturb and seize it as well.[177]And, in *Jones* both territorial and informational privacy interests were implicated by the physical attachment of the GPS device to the defendant's car from which information was collected and used to support criminal charges.

While this next generation of technologies certainly adds a new dimension to informational privacy, its use implicates the interests we have in limiting intrusions into our spatial domains and movements so as to be free from observation in even more profound ways than have previously been the case. Privacy has both spatial and informational dimensions, but "linking privacy to informational transparency tends to

---

[174] *Ibid* at para 50.

[175] *Ibid*.

[176] *Ibid* at para 45.

[177] *Ibid* at para 55.

mask a conceptually distinct harm that is spatial."[178] Analytical approaches that characterize privacy interests as informational, even when a territorial interest is also implicated, put the privacy interest in a less protected category.[179] Further, this approach risks spatial interests being collapsed into the informational paradigm. This would further marginalize these core interests, already being narrowly interpreted under the territorial construct, thus weakening the overall privacy protection framework. Informational inaccessibility is not enough. The proposed new conceptual construct, 'peopled places,' developed in later chapters, addresses these limitations.

The problems associated with the zonal classification scheme are exacerbated by the cases not being clear about how the relevant factors are supposed to contribute to a finding concerning a reasonable expectation of privacy because there are two different strands of arguments at work. On the one hand is an ends based judicial approach that focuses on the security of the place, or information searched, from intrusion by the world at large.[180] If the place searched is not in fact secure against the world in general, then it is not secure against government agents in particular and thus, any expectation that the state will not intrude is not reasonable. In other words, the accused, by failing to adequately secure his or her interests against intrusion from the world at large, is deemed to have accepted the potential intrusion on his or her privacy interests and so cannot complain if the person who intrudes happens to be an agent of the state. Thus, questions of the ease or difficulty of physical access and of whether the accused should be deemed to have waived or abandoned her privacy are central to the court's analysis.

For example, this approach is illustrated by the reasoning and outcome in *Edwards* and *Patrick*. In *Edwards*, the court held that the accused had no reasonable expectation in his girlfriend's apartment. He could not control access to the apartment as he was, on the factual findings of the courts, "no more than an especially privileged

---

[178] Cohen, *Configuring the Networked Self*, *supra* note 11 at 138.

[179] Jane Bailey, "Framed by Section 8: Constitutional Protection of Privacy in Canada" (2008) 50:3 CJCCJ 279-306 at 302.

[180] For example, *Edwards, supra* note 126; *Patrick*, *supra* note 21.

guest" in the apartment."[181] Why do these facts matter? The underlying idea seems to be that because he "could not be free from intrusion or interference in his [girlfriend's] apartment by the world at large, he could not object to intrusion or interference by the police. The accused could not prevent his girlfriend, or a stranger, from discovering evidence against him in the apartment and turning it over to the police. Thus, he took the risk that the evidence would be discovered so he could not complain if the intruder was a police officer, even if the officer's search of the girlfriend's apartment was blatantly unlawful.[182] Similarly, in *Patrick*, the accused was found to have no reasonable expectation of privacy in bags of garbage left on his property, near the property line, for pick-up. Although the garbage amounted to "bag[s] of information" that could reveal a great deal about the accused's activities within his home,[183] and although there was a municipal by-law that prohibited anyone other than the garbage collectors from taking it,[184] the accused was deemed to have abandoned any expectation of privacy he might otherwise have had in the bag. Anyone could have picked it up, lawfully or not.[185] That the garbage was picked up by the police, not a homeless person or animal, was just a risk that the accused took.

A second approach, on the other hand, is more value-based, the focus of which is on whether a reasonable person would anticipate that an agent of the state would be able to intrude on the accused's privacy interests with no specific legal authority to do so. The central question is whether the investigative technique at issue intrudes on privacy in a manner that raises constitutional concerns about its unfettered use. Here, the most important factors typically relate to the impact of the technique on the values protected by the privacy interest. This approach is illustrated in the Supreme Court's cases on electronic surveillance,[186] For example, in *Duarte*,[187] the police installed

---

[181] *Edwards, ibid* at para 47.

[182] *Ibid* at para 51. The majority does not decide whether the search was unlawful. They hold that the accused could not object to it under section 8 even if it was unlawful. Justice LaForest concurring in the result, thought that the search was best described as a "constructive break-in" (at para 69).

[183] *Patrick*, *supra* note 21 at para 30.

[184] *Ibid* at para 68.

[185] *Ibid* at para 55.

[186] See for example, *R* v *Duarte* [1990] 1 SCR 631 [*Duarte*]; and *Wong, supra* note 144.

recording equipment in an informer's apartment. A conversation among the accused, the informer, an undercover officer and others was captured by this equipment. The making of the recording was lawful under the *Criminal Code* because the informer had consented and both the informer and the officer could have testified at trial to the content of their conversations with the accused. Nonetheless, the majority of the Supreme Court held that the accused had a reasonable expectation that his conversations would not be recorded without judicial authorization. If such an expectation was not recognized, the state would have an unfettered power "to make permanent electronic recordings of our private communications." Justice LaForest was concerned about the invasiveness on the private sphere of unrestricted recording of private conversations. "No set laws" he wrote can protect us from the risk "that their interlocutors will divulge communications that are meant to be private."[188] But electronic surveillance presented "the much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words."[189] The question then is whether any given intrusion should be permitted without legal authorization, in light of the inhibiting effects of the intrusion on the activities protected by privacy.

The lack of a robust and coherent model of privacy became evident in *Tessling*. In certain respects, *Tessling* involved a straightforward application of the principles in *Plant* and *Edwards*. However, the case required the court to confront the state's use of a relatively new technological technique to interpret emanations of heat from within a protected sphere of privacy and as such, *Plant* and *Edwards* did not fit in the context of the facts in *Tessling* since there was no physical intrusion. Binnie, while acknowledging the territorial interest associated with the home, adopted an informational analysis. In assessing the scope of the interest,

Binnie concluded that the assessment had to be made with reference to the actual, as opposed to theoretical, potential of the technology at issue, and that the

---

[187] *Edwards, supra* note 126.

[188] *Ibid* at para 21.

[189] *Ibid* at para 22.

nature of the information it revealed was the key. Because FLIR technology revealed information that "is only as helpful as the inferences it is capable of supporting" and the heat emanations are, on their own, "meaningless", he concluded that there is no reasonable expectation of privacy in the information to be gleaned from heat emanations "off the wall" of our homes. He specifically declined to fix "bright-line" applicable to future technologies and preferred instead to focus the analysis on the reductionist nature and quality of the information made available by the then current incarnation of FLIR technology.[190]

Justice Binnie's decision says that current technology cannot 'see' what is happening in the home because it cannot reveal the cause of uneven heat distribution. This points to the problem of drawing analogies to human surveillance abilities to justify technologically enhanced surveillance capabilities, suggesting 'visibility' is only a privacy harm when it is actual physical seeing. In other words, Justice Binnie's 'seeing' analysis does not sufficiently consider technologically-mediated visibility as a legitimate privacy harm. Greater visibility created by observation can include visual images and information gathering. Or as Julie Cohen characterizes, the spatial dimension of the privacy is an interest in avoiding or selectively limiting exposure.[191] This would encompass the operation of non-visual mechanisms designed to render individual identity, behaviour, and activities transparent.

Justice Binnie also chose not to use *Tessling* to regulate FLIR technology, but explains that should the technology arrive where the state can see into the home, the findings of this case would be open to revision. This is problematic for the reasonable expectation of privacy test and future technologies. For example, assuming that RFID technology will become ubiquitous, and that many RFIDs will remain activated, our ability to use this advancing technology will reduce our expectations of privacy. It will enable increasing, systematic and covert localization of individuals on a much wider scale. This substantially impacts people's traditional reasonable expectations of privacy in movement: they may have been visible at a certain time at a certain place,

---

[190] Kerr & McGill, *supra* note 169 at 412-424.

[191] Cohen, "Privacy, Visibility, Transparency, and Exposure" *supra* note 61.

but much less traceable for a longer period of time. The overall result is that more of our lives, in more places, are exposed. The reasonableness of our privacy expectations in movement is diminished the more localization becomes a common side-effect of technology. It is not difficult to reduce reasonable privacy expectations by first eliminating the privacy, then the expectation of that privacy and, last, the reasonableness of our expectation of privacy. If society has no subjective expectation of privacy, because in fact, it has no privacy, then any claim to privacy would be objectively unreasonable to society as a whole. The eroding effect of technology on privacy is a slow, hardly perceptible process. There is no precise stage at which one can point to the use of technology as unreasonably tilting the balance of privacy. However, because of the fluid and flexible nature of privacy, society has been and will continue gradually to adapt to new technologies and to the diminished privacy expectations that go with them. Justice Binnie's technology assessment with respect to FLIR, although well-intentioned, does not take longer term implications into account. Moreover, what Justice LaForest described as the "syllogistic reasoning" this type of analysis entails is problematic both for its failure to articulate a theory of privacy capable of producing more predictable results in future cases and for the extent to which the existence of a reasonable expectation of privacy becomes contingent on property rights.

4. *R v Jones* in Canada

Recall at the beginning of this chapter in *Jones*, the Supreme Court of the United States held that the warrantless use of a GPS tracking device affixed to the defendant's car amounted to a search for the purposes of the Fourth Amendment. The court based its decision on a literal reading of the Fourth Amendment emphasizing that the case presented a situation in which "[t]he government physically occupied private property for the purpose of obtaining information," and therefore, was trespassory in nature.[192] Justice Alito concurred in the result, but wrote that he would have analyzed the case

[192] *Jones*, *supra* note 2 at 949.

within the reasonable expectation of privacy test, suggesting that short term monitoring may be one that society recognizes as reasonable, but the "long-term monitoring and tracking" violated the defendant's Fourth Amendment rights because it "involved a degree of intrusion that a reasonable person would not have anticipated."[193] The significance of the case is, first, that all electronic surveillance cases involving a trespass upon property should be deemed a search, and second, that all other cases that do not involve a trespass, will still be subject to the *Katz* reasonable expectation of privacy analysis.

In Canada, the Supreme Court considered the same issue, some 20 years ago with far less sophisticated tracking technology in *R* v *Wise*.[194] An electronic tracking beeper was installed in the defendant's car after the expiry of the warrant for about four months. The court agreed that the physical installation of the device without a valid warrant violated section 8, but it split in its approach with respect to the reasonableness of the privacy intrusion in the subsequent monitoring. Writing for the majority, Justice Cory, found the search was only minimally intrusive on the basis that the vehicle was travelling on public roads, the device was attached to the car and not the accused, and the device used was an unsophisticated rudimentary extension of physical surveillance based on its lack of sophistication. Accordingly, the admission of evidence in this case (the subsequent warrantless monitoring) would not bring the administration of justice into disrepute.[195]

Justice LaForest dissented, finding that the installation of the tracking device constituted an unlawful trespass *and* violated his rights under section 8 because an individual has a reasonable expectation of privacy in his movements, even when travelling on a public road. For Justice LaForest, "the crucial point is that there is a

---

193 *Ibid* at 964.

194 *Wise*, *supra* note 143.

195 Section 24(2) under the *Charter* provides that where "a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by theis Charter, the evidence shall be excluded if it is established, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute."

The outcome in *Wise* of a s.24(2) analysis appears to add another dimension by allowing the court to find a privacy violation, but then determine that it is essentially trivial or immaterial. It is beyond the scope of this thesis to consider the role this type of potential escape hatch plays in the privacy analysis.

qualitative difference between the risk that one's movements in a car will be observed by others, including authorities, and the risk that one's vehicle will be monitored by a device that follows its every movement."[196] Neither does Justice LaForest accept Justice Cory's 'unsophisticated technology' reasoning, arguing that the decision in this case should regulate the use of tracking technologies more generally because this technology will likely develop well past what is currently available, through which surveillance can occur without the need to physically or visually monitor. Unlike *Tessling* – and by implication Justice Scalia's opinion in *Jones* – for LaForest, Justice Cory's assessment does not take into account the implications of the technology.

What then would be the result if the *Jones* scenario was in front of the Supreme Court of Canada? A trespass test is unlikely to even arise, given the progress of tracking technology, but, on the basis of *Duarte* and *Wise*, longer term, and potentially shorter term, monitoring may be a violation of the reasonable expectation of privacy if information is obtained as a result of the monitoring. There are difficult "thorny" questions that follow: What is the nature and extent of the information obtained from the tracking device? Whether or not an individual has a reasonable expectation in that information? Does an individual maintain a reasonable expectation of privacy in information that she voluntarily discloses via, for example, OnStar, networked cell phones, social media, location-based services or embedded everyday devices. These issues are addressed by the new peopled places construct as illustrated in Chapter Five.

5. Conclusion

This chapter canvassed the conceptual and legal privacy landscape. In terms of the conceptual underpinnings of privacy, emerging technologies are creating privacy issues that appear to fall outside the bounds of traditional exclusionary analysis informing constitutional search doctrine. The examination of the dimensions of

[196] *Ibid* at para 80.

privacy, or the zonal approach to privacy interests, revealed that each privacy interest, personal, territorial and informational, has been narrowly interpreted, which fails to take into account the nature of changing technologies. Moreover, these interests often overlap, which has led to a different set of problems that undermine protection of spatial privacy. The scope of reasonable expectation, as explored under section 8 jurisprudence, reinforced a need to overhaul the territorial model of privacy.

The scope of the territorial zone of privacy, as interpreted by the Supreme Court of Canada, has largely remained tied to its territorial roots by focusing on a defined, and often bounded, physical location or place under surveillance. The effect has been to further entrench a property analysis despite the pronouncement that *Hunter* "ruptured the shackles of that confined [search and seizure] claims to property."[197] The cases since *Hunter* have not found a way to put the aspiration of moving beyond trespass theory into a framework for protecting the spatial dimension of privacy beyond traditional property principles. The difficulty is compounded by the ambiguity of the now-famous phrase used to reject the proprietary basis for privacy protection, privacy protects "people not places."[198] Presumably, it meant privacy was to be applied to protect people rather than just places. In other words, the court rejected the 'sole' requirement of physical trespass refocusing its analysis to recognize the protection of people. The *Jones* decision in the United States supports this reading of the phrase 'people not places' in adopting the trespass test in that case.[199] Yet, it is unclear how the territorial notion of privacy protects people except to the extent of being 'in' places, and the interpretation given to 'place' is one that adheres, historically and conceptually, to the public-private distinction. This is consistent with the inside/outside approach, or Justice Scalia's description, "off-the-wall" rather than "through the wall" which avoided having to address, head-on, the issue of the

---

197 *Dyment*, *supra* note 20 at 428.

198 *Hunter*, *supra* note 118 at 145.

199 *Jones*, *supra* note 2 at 952. While recognizing that the most of its recent Fourth Amendment decisions have been based on a defendant's reasonable expectation of privacy, the Court noted that this approach, first articulated in *Katz,* never supplanted the core trespassory analysis. As Justice Scalia explained, "the-reasonable-expectation-of-privacy-test has been *added to*, not *substituted for*, the common-law trespassory test."

reasonableness of a person's expectation of privacy in the home where there is no physical trespass. The same issue left open by the Supreme Court of the United States in *Jones*, albeit in the context of a private vehicle rather than the home. Moreover, deprived of the boundary lines provided by place as traditionally defined, courts resort to factors that weaken privacy protection rather than bolstering it. By examining whether the nature and quality of the information sufficiently meets the low threshold to warrant section 8 protection lends itself to decisions that require controversial judgments about what activities people should and should not have a right to shield from others.

One way to address the inadequacies identified in this chapter is to build a new conceptual construct of territorial privacy that can sustain effective legal protection in response to the spatial risks arising from ubiquitous computing. This dissertation rejects the current analytical benchmark of privacy protecting 'people not places.' Instead, it proposes and develops the conceptual and legal construct of 'peopled places' in which to formulate a framework for protecting people *and* places. In order to give effect to protection of 'peopled places', it means moving beyond the zonal approach and beyond narrow interpretations and naïve perceptions of 'place' as bounded or defined geographical territory. It requires developing a new conceptual construct of 'place', one that better reflects the spatiality central to our experiences and expectations in everyday life. The first step in this building process is to have a clear understanding of what place means and an adequate foundation for building a new construct. This enquiry is taken up in Chapter Four: 'What is Place' which explores the meaning of place as it is currently applied in law and key perspectives taking an alternate approach to conceptualizing place.

CHAPTER FOUR

WHAT IS 'PLACE'?

> *When everything else has gone from my brain – the President's name, the state capitals, neighbourhoods where I lived, and then my own name and what it was on earth I sought, and then at length the faces of my friends, and finally the faces of my family – when all has dissolved, what will be left, I believe, is topology: the dreaming memory of the land as it lay this way and that.*
>
> Annie Dillard, *An American Childhood* (1987)

1. Introduction

In 1967, the United States Supreme Court declared that the Fourth Amendment "protects people and not places."[1] The Court agreed with Charles Katz that even though he was not in his home, he expected that any conversation carried on in a telephone booth would be private. *Katz* is a significant decision. In departing from the trespass theory for assessing Fourth Amendment search cases, concurring Justice Harlan articulated a new standard for determining whether the state had conducted an unreasonable search. The new test, the reasonable expectation of privacy, has since been consistently employed by both American and Canadian courts. However, what has largely been lost is Justice Stewart's majority opinion, the focus of which was on whether a telephone booth was, like the home, a constitutionally protected area. This raises the question of whether Justice Stewart meant to say privacy protects people *and* places, or people in places, rather than people *not* places.

In *Katz,* the court held that even though the defendant was not in his home, he expected the telephone booth setting would be private. Hence, a constitutionally

---

[1] *Katz v United States*, 389 US 347 (1967) [*Katz*], expressly adopted by the Supreme Court of Canada in *Hunter v Southam Inc*, [1984] 2 SCR 145 [*Hunter*].

protected place. It has been suggested, therefore, that the United States Supreme Court was actually "claiming that as technological changes occur, society needs to recognize that the places within which people carry out their lives also change. If in the past the paradigmatic private place was the home, now it may be a telephone booth."[2] Yet, both American and Canadian courts have seemingly struggled with technological changes and how these changes may influence and reconfigure places; in particular, private places. Thus, courts have largely remained tied to a traditional notion of place – a geographic, fixed and bounded physical space. It is a "view where a region may be a place, and a town, a suburb, and a house, but not a telephone booth. It is a view that takes as natural and given the existence of places of particular sorts and scales, and renders the rest invisible."[3] A view, in other words, that sees the world in terms of a grid or map, on which like places are located. And further, some of these locations can be categorically private places or public spaces, as traditionally understood.

This is problematic for privacy law because, as discussed in Chapter Three, while early constitutional privacy cases held promise for protecting people and places,[4] the more recent Supreme Court privacy jurisprudence suggests a view of the world in which place is hierarchical and structured.[5] Taking this narrow approach to place, people and information are safeguarded by determining whether police physically entered a private place. When instead, if, as the Supreme Court of Canada has proclaimed, people have the right to be left alone,[6] the question should be, does the state action violate this right. It is, according to Supreme Court of Canada Justice LaForest (as he then was), the values of a free and democratic society that are to provide the content for an independent justification for privacy.[7] By assessing place as

---

[2] Michael Curry, "The Power to Be Silent: Testimony, Identity, and the Place of Place" (2000) 28 Historical Geography 5-16 at 17.

[3] *Ibid.*

[4] See for example, *R v Duarte*, [1990] 1 SCR 30 (LaForest); *R v Wong*, [1990] 3 SCR 36 (LaForest); *R v Wise*, [1992]1 SCR 527 (LaForest Dissent).

[5] See for example, *R v Tessling 3 SCR 432 [Tessling]*; *R v* Gomboc, [2010] 2 SCR 211; *R v Patrick*, [2009] 1 SCR 579.

[6] *Hunter*, *supra* note 1; Samuel Warren & Louis D Brandeis, "The Right of Privacy" (1890) 4:5 Harvard Law Review 193-220.

[7] *Duarte*, *Wong* and *Wise*, *supra* note 4.

a spot in the world and people as merely located at that spot contributes to the erosion of privacy. Consequently, it becomes increasingly difficult to support a conception of place by which people are able to develop their identities and self.[8]

The changing nature of computing technologies renders these issues associated with the construction of place even more important. Ubiquitous computing is based on technological developments that make it possible to embed powerful computational elements and digital components into everyday objects, portable devices and the built environment. This trend is inducing significant changes not only in the development and implementation of new technology, but also on the relationships between interactive systems and their users. Distributing computational power within an environment and its objects and places means we are no longer concerned solely with people's interaction with the desktop computer, but now with the physical environments that people experience through their daily lives. People will encounter technologically enhanced spaces, places and artifacts as they move through a variety of environments. These systems will be able to respond and react to their presence and actions. Current approaches in law, policy and scholarship to emerging technologies represent a tendency to focus so much on information flows, that it is forgotten that when information flows, it flows through the places of our everyday lives. Bringing technologies beyond the desktop and into the everyday world requires us to pay greater attention to the physical environment where the interaction occurs. And this requires us to deepen our understanding of the central concepts of space and place.

Effective legal protection of territorial privacy rests fundamentally on the ability of law to invoke a more adequate conception of place. Traditional geographical conceptions of place constrain the legal construct because in general they have not accounted for the richness of personal, social, cultural and material aspects of context. The problems with privacy theory and practice are, to some extent, a reflection of law's

---

[8] Jeffrey Reiman, "Privacy, Intimacy and Personhood" in Ferdinand Schoeman, ed, *Philosophical Dimensions of Privacy, An Anthology* (Cambridge, UK: Cambridge University Press, 1984) 300-316; Edward Relph, *Place and Placelessness* (London: Pion, 1976); Irwin Altman & Setha Low, eds, *Place Attachment*, (New York: Plenum, 1992); David Cantor, "The Facets of Place" in Gary T Moore & Robert W Marans, eds, *Advances in Environment, Behaviour and Design* (New York: Plenum, 1997) 109-148;.Twigger-Ross & D Uzzell, "Place and Identity Processes" (1996) Journal of Environmental Psychology 16.

failure to draw on other perspectives for a theoretical conception of 'place' that better captures the spatiality central to our everyday lives. A multi-disciplinary approach to 'place' seeks to leverage the law's lost opportunities. If privacy is to protect people, it must protect them in their lived spaces, a place that is not necessarily bounded, merely defined as a location or grounded in proprietary principles. To see people as agents of place, and that it is ultimately people that give place meaning. This would not only understand places as people truly experience them, but also come closer to fulfilling the *Katz – Hunter* aspiration of protecting the privacy of people rather than be determined largely on the basis of physical exclusion from the King's castle.

Therefore, this chapter seeks to further our understanding of 'place' by drawing on key perspectives within the larger phenomenological tradition that better captures our lived experience in the physical world. The objective is to provide a conceptual foundation upon which to build a new model of territorial privacy. This discussion is mainly expository, outlining a set of arguments drawn from theorists that will inform Chapter Five. While the focus of this chapter is to explore the meaning of place for the purpose of proposing a broader meaning of 'place' than found in traditional accounts, the concept of 'space' still matters. The Euclidean, or Cartesian, concept of space matters to the extent that it informs mobility and surveillance analysis,[9] cyberspace literature contesting space and place,[10] and law.[11] However, as this chapter sets out, the concepts of space and place must be more carefully and more broadly understood. The historically entrenched concept of uniform, metric physical space is not entirely adequate for a privacy framework because it fails to capture features of our lived

---

[9] Colin Bennett & Priscilla Regan, "Surveillance and Mobilities" (2004) 1:4 Surveillance and Society 449; Mimi Sheller & John Urry, eds, *Mobile Technologies of the City* (London, UK: Routledge, 2006); Tim Cresswell & Peter Merriman, eds, *Geographies of Mobilities: Practices, Spaces, Subjects* (Burlington, VT: Ashgate, 2011); Adrianna de Souza e Silva & Jason Firth, "Locational Privacy in Public Spaces: Media Discourses on Location-Aware Mobile Technologies" (2010) 3:4 Communication, Culture & Critique 503-525.

[10] John Perry Barlow, "A Declaration of Independence in Cyberspace" (1996), online: Electronic Frontier Foundation <http://projects.eff.org/~barlow/Declaration-Final.html>; David R. Johnston & David Post, "Law and Borders: The Rise of Law and Cyberspace" (1996) 48 Stan L Rev 1367; Dan Hunter, "Cyberspace as Place and the Tragedy of the Digital Anti-commons" (2003) 91 Cal L Rev 439; Mark Lemley, "Place and Cyberspace" (2003) 91 Cal L Rev 521; David McGowen, "The Trespass Trouble and the Metaphor Muddle" (2005) 1 JL Econ & Pol'y 109.

[11] Jane Holder & Carolyn Harrison, eds, *Law and Geography* (Oxford, UK: Oxford University Press, 2003); and see for example *R v Dyment*, [1988] 2 SCR 417 [*Dyment*]; *Tessling*, *supra* note 5; *Patrick, supra* note 5.

spaces that characterize, and are critical to, contemporary life and everyday interactions. Chapter Four concludes by proposing a spatial conception that works alongside the geometric and structural elements of our environment. It adopts an experiential conception of place as primarily developed within humanistic geography, a field that studies how humans interact with space and their physical and social environments. While acknowledging the continued significance of space as structural, the humanists' commitment to people and their making of place based on the 'lived nature' of spaces in the real world serves as a strong conceptual grounding for building a new spatial construct to sustain privacy. An experiential conception of place addresses the current normative limitations by taking account of the different ways a space may be understood and used, as well as what characterizes ubicomp; the embodied and tangible interaction in the physical environment. The formula for a new conceptual construct, therefore, is human-centered-computing plus humanistic-place, which equals 'peopled places.' The conceptual construct of peopled places is defined and developed in Part One of Chapter Five. In Part Two of Chapter Five, the peopled places construct is applied in law to demonstrate how it more effectively protects spatial privacy interests.

2. Space {and/versus} Place

Like the concept of privacy, the concept of place is notoriously complex, described as "the most elusive of concepts…conceived and debated over time by a wide range of theorists and critics."[12] For Jody Berland, it "has become one of the most anxiety-ridden concepts today."[13] And for Nigel Thrift, "the nature of place is anything but fully understood." [14] Defining exactly what place is turns out to be very difficult

---

[12] Rowan Wilken and Gerard Goggin, *Mobilizing Place*, (New York: Routledge, 2012) 4.

[13] Jody Berland, "Place" in Tony Bennet, Lawrence Grossberg & Meagan Morris, eds, *New Keywords: A Revised Vocabulary of Culture and Society*, (Oxford: Blackwell, 2005) 256-258, 257.

[14] Nigel Thrift, "Space: The Fundamental Stuff of Human Geography" in Nicolas Clifford, et al, eds, *Key Concepts in Geography*, (London: Sage, 2009) 85-96, 91.

since place is everywhere, but nowhere defined.[15] Basic dictionary definitions do little to resolve the lack of definitional clarity and precision and in fact reflect the complexity of the word place.[16] Despite these challenges, thematic signposts can be identified, the first of which is the (dis)entanglement of the concepts of space and place.

2.1 Common Understandings

It is difficult to critically think about 'place' without also considering the concept of 'space.' Indeed, any philosophical discussion about ubiquitous computing and spatial privacy necessitates comparing space and place. Yet the distinction between them is not always clear.[17] At first, intuitively, it may seem to be fairly straightforward to distinguish between space and place; the world is a world of places within space. But this obviously begs the question of what do these concepts mean since for words such as space and place "there exists far reaching uncertainty of interpretation."[18] Take as a simple example, two people looking out at the ocean, one may see it as a 'place' to go, while the other sees it as a vast open 'space.' Travel writer Jonathan Raban makes a similar point in his account of explorer Captain Vancouver's journey along the west

---

[15] Edward Casey, *Getting Back Into Place*: *Toward a Renewed Understanding of the Place-World,* (Bloomington, IN: Indiana University Press, 1993) and *The Fate of Place: A Philosophical History,* (Berkeley, CA: University of California Press, 1997).

[16] There are around three and a half pages to definitions of place ranging from broad references to space and its occupation of these spaces to different types or subcategories of geographical space including a residence or dwelling, a town square, a village, a city, area or region to an area with definite boundaries to a setting at a table to a spot on the body to a particular circumstance, role or status: *Oxford English Dictionary,* 2nd ed, sub verbo "place".

[17] Once you get beyond space in its formal and most familiar sense, reviewing space and place discourse is a daunting exercise. The seemingly infinite types of spaces and many dimensions of space and place that have been examined by a multitude of disciplines appear to be layered upon one another or contained within the next, and interwoven with other concepts. Much of the literature underscores what might be described as a tension between space and place: See for example, Edward Casey, *The Fate of Place* and *Getting Back Into Place, supra* note 15; Henri Lefebvre, *The Production of Space* (Oxford, UK: Blackwell, 1991); David Harvey, "From Space to Place and Back Again" in Jon Bird et al, eds, *Mapping The Futures* (London: Routledge, 1993) 2; Jeffrey Malpas, *Place and Experience: A Philosophical Topography* (Cambridge: Cambridge University Press, 1999); Edward Relph, *supra* note 8; Michael Curry, "Discursive Displacement and the Seminal Ambiguity of Space and Place" in Leah Lievrouw & Sonia Livingstone, eds, *The Handbook of New Media* (London: Sage Publications, 2002) 503-517.

[18] Albert Einstein quoted in Max Jammer, *The Concepts of Space in Physics*, 3rd ed, (Toronto, ON: General, 1993) xiv.

coast of North America.[19] Raban, while travelling himself along the coast, tells the story of Captain Vancouver being puzzled at the way the natives navigated their canoes in the ocean around them, seemingly taking more complicated routes than was necessary But, for the native canoeists the routes they took made sense to them because they navigated the ocean as a set of places based on spirits and dangers. Rather than vast blank open space as seen by Captain Vancouver, the natives looked at the sea and saw place: "[t]wo world-views were in collision; and the poverty of white accounts of these canoe journeys reflect the colonialists' blindness to the native sea. They didn't get it – couldn't grasp the fact that for Indians the water was a place, and the great bulk of the land was undifferentiated space."[20]

Such uncertain interpretations are reflected in our everyday language. Space and place are familiar words, often used directly or indirectly. For example, 'have you got space for this?' or 'will my car fit in that parking space?' or 'you are invading my space.' We live in space, move through it, explore it, navigate it, manipulate it and defend it. Space might refer to a room, the view outside the kitchen window, what is between two chairs, or what is left behind when something is moved. Space then means different things in common usage, but it is also used with such ease that its meanings run into each other, and to a certain extent, taken for granted. Similarly, think of the ways 'place' is also used in everyday speech. For example, announcing 'dinner is at my place tonight' suggests some kind of proprietary connection between a person and a particular location or physical setting. We have to be somewhere and to be somewhere is to be in some kind of place. It also suggests a notion of spatial privacy, belonging and control as 'my place' is not 'your place.'

Like Creswell's university dorm, recall moving into an apartment or house. You have a particular area of space with the basic appliances and perhaps some fixtures, most of which do not mean so much to you. Yet, this essentially blank space

---

[19] Jonathon Raban, *Passage to Juneau: A Sea and Its Meanings*, (New York: Pantheon Books, 1999) as cited and described by Tim Cresswell, *Place* (Malden, MA: Blackwell, 2004) 8-10.

[20] Raban, *ibid* at 103; cited by Cresswell, *ibid* at 9.

presumably meant something to other people and now you will make the space say something about you by adding your own possessions, putting pictures on the wall and creating memories by interacting with others in that space; "thus, space is turned into place, your place." Viewed in this way, space is a more abstract concept whereas place is somewhere and has content. Moreover, this example reflects how the fundamental use of space turned into place concerns human territoriality, or territorial space, a key theoretical underpinning informing the legal protection of privacy.

The term territory generally refers to a particular or indeterminate geographical area. Territorial space is the physical manifestation of something, namely, a physical location.[21] Territoriality is the means of exercising control over this physical space or place.[22] Although a territory is not synonymous with property, territoriality works to control defined spaces and physical places or locations. Thus, territorial space finds architectural and geographical expression whereby control over access serves as a defensible shield to protect privacy. This largely translates, as shown in Chapter Three, into invasions of privacy rooted in trespass theory.

Spatial dimensions of our lives, however, involve not only constructions of territory anchored in physical space, but also establishing personal zones of privacy.[23] People often expect space from others, even when they are with other people or when in public. Personal space has been defined as "an area with invisible boundaries surrounding a person's body into which intruders may not come."[24] Personal space differs from other territories in that it is portable, but emphasizes distance for the

---

[21] Byran Lawson, *The Language of Space* (Oxford: Architectural Press, 1999) 164-191.

[22] Julian Edney, "Human Territoriality" (1974) 81 Psychological Bulletin 959.

[23] Robert Sommer, *Personal Space: The Behavioural Basis of Design* (Englewood, NJ: Prentice Hall, 2008); ET Hall, *The Hidden Dimension* (Garden City, NY: Doubleday, 1969); Georg Simmel, "The Metropolis and Mental Life" in D Levine, ed, *On Individuality and Social Forms* (Chicago: University of Chicago Press, 1971).

[24] Hall, *ibid* at 122.

purposes of exclusion from others.[25] Personal space, and hence a personal zone of privacy, takes on greater significance when considered in the context of ubiquitous computing since it operates across physical territories, as does technology-enhanced surveillance without physical intrusion.

In the same way as space can become place through the process of territoriality, place gains meaning though the process of naming and visualization of that place. As geographer Tim Cresswell points out, to most longitude and latitude coordinates would not mean so much.[26] For example, 42°21'29"N71°03"49"W for many likely indicate a location of some sort, but not much more than a set of numbers indicating a location somewhere without meaning.[27] These coordinates are for the city of Boston, which then might bring to mind, Harvard University, Boston Common, Faneuil Hall, or Fenway Park. Replacing the coordinates with an actual name in which we can visualize and associate sites with that name is closer to being a place than a point in space somewhere. Hearing that a bomb exploded at 42°21'29"N71°03"49"W would not have the same impact as hearing that it exploded in downtown Boston. Moreover, the space of the city is turned into the place where the Boston Marathon finished, and now, horrifically, the place where the bombs exploded.

In conducting our practical affairs we seem to take for granted that people, places, objects and events are spatially distributed. We have a natural awareness that space is an organizational feature of sorts of our daily lives, embedded within practical matters such as 'how far is Sudbury from here?', 'where is the nearest bathroom?' or 'what is the quickest way to Kettleman's Bagel Shop?' Initially, space is not some worldly abstraction, but integral to the accomplishment of the activities we do. Spaces and places become, as it were, the settings within which activities of various kinds

---

[25] *Ibid*. *R* v *Dyment*, [1988] 2 SCR 417 at para 21 [*Dyment*], LaForest J. refers to a spatial realm that "transcends the physical and is aimed at protecting the dignity of the human person".

[26] Cresswell, *supra* note 19 at 2.

[27] The same can be said for IP addresses. The set of numbers themselves will not mean much to most people, but the name, tangible, or visual representation will give some degree of meaning to the internet address. For example, the IP address 137.122.14.11 does not necessarily trigger anything meaningful to most, but likely would for many once it was known to be uottawa.ca. Similarly, bar code numbers or postal codes, although most know can identify at least the provincial location from the first letter of the postal code.

occur.[28] These practical actions are what constitute our everyday reality in the real world, one that is spatially organized and materially structured. This is consistent with the observation that certain spaces or places are tied to the performance of particular activities. For example, classrooms are organized for teaching, restaurants for eating, libraries for storing and retrieving books and roads for driving. There is a sense, then, that particular spaces or places are tied to particular activities; that spaces and places are institutionalized, and as such, constrain and shape action.[29]

All of these general common-sense notions of space and place are important for two main reasons. First, vernacular understandings of space and place underpin many theoretical understandings. However, beyond the ostensive identification of space and place, the theoretical landscape is extraordinarily vast, and ultimately, the distinction between space and place "is one of the best kept secrets in spatial theory."[30] Much of the discourse on spatial theory oscillates between visions of space and place in ways that complicate drawing any sharp and easy divisions between these concepts.[31] There is a connection between space and place, but it is, in lineage and across disciplines, one of complexity and "discursive displacement."[32] It is, then, important to keep in mind that the concepts of space and place are closely intertwined. Second, this dissertation seeks to provide a more effective basis for the legal protection of privacy. A person's reasonable expectations are central to this legal determination. Our understandings or perceptions of space and place factor in to these expectations. Our understanding of a place or space will, in part, affect the privacy expectations we have. The remainder of this chapter looks at key themes in spatial thinking, followed by alternatives to the way space and place are characterized in traditional theories.

---

[28] Erving Goffman, *Asylums* (New York: Doubleday, 1961) 11-17.

[29] *Ibid*.

[30] Casey, *supra* note 15 at 270.

[31] See *supra* note 17.

[32] Curry, *supra* note 17.

2.2 Theoretical Underpinnings

Investigating the meaning of place cannot be done but in conjunction with an understanding of the notion of 'space' derived from the classic and scientific traditions. This section provides a brief sketch of how place has been characterized within these traditions, the purpose of which is to help explain current legal approaches to territorial privacy and reinforce the need for a broader conception of place than is employed in law. Following this overview, an alternative perspective on the notion of place is introduced and discussed.

The early philosophical history of the concept of space is dominated by ambiguity of Greek spatial terms. The Greek language did not have a one-word equivalent to 'space.' Instead, space was discussed within the classical ideas of "choras" (region) and "topos" (place).[33] Within this analysis, the nature of space is based on the fundamental association between being and place as "to be (at all) is to be in (some) place."[34] For Plato, space was empty, a receptacle for being whereas Aristotle understood space as the 'place' of being.[35] Aristotle defined place as a container or boundary for an object, a "reservoir of physical possibilities" in which things and people move in and through.[36] Place has its unique and non-reducible features which cannot be replaced by measurable space because "what matters most is not the measurement of objects in empty space, but the presence of sensible things in their appropriate and fitting places."[37] In other words, space is static, hierarchical, and concrete, a world where things and people have places where they belong.

---

[33] For a detailed study on these concepts, now considered traditional forms of inquiry in geography, see Keimpe Algra, *Concepts of Space in Greek Thought* (Leiden, Netherlands: Brill, 1995). See also, Tim Cresswell, *Geographic Thought: A Critical Introduction*, (West Sussex, UK: John Wiley & Sons, 2013) 14-33.

[34] Casey, *supra* note 15 at 4.

[35] Michael White, "Aristotle on the Infinite, Space and Time" in Georgios Anagnostopoulos, ed, *A Companion to Aristotle* (Oxford, UK: Wiley & Sons, 2009) 260.

[36] *Ibid* at 265.

[37] Casey, *supra* note 15 at 71.

Today various models for all kinds of spaces are discussed without realizing that this is a distinctly modern way of thinking.[38] Geometrical traditions did not directly think about different kinds of space, a conception of space or even space itself, but instead, the scientific properties of space. Euclidean space, or the Newtonian view of space,[39] is a mathematical model, the boundless three-dimensional extent in which objects and events occur and have relative position and direction.[40] In other words, space is absolute, understood qualitatively empty, immobile, homogenous and an infinite expanse in which everything is located. [41] Others within the scientific tradition characterize space as relational. Gottfried Leibniz argues, as did Aristotle, that we need to attend to the relationships among objects and events to the extent that we come to see space as fundamentally relational and defined entirely in terms of those relationships.[42] If all objects were removed from space, if space were completely empty, it would be as "meaningless as an alphabet that is missing its letters."[43]

Traditional geographical ways of thinking about space share a common underlying mathematical image of the world with classic philosophical and scientific traditions.[44] Pure geographical space is seen as an empty container, and places as simply locations within space. The grid is a conceptual tool for defining space, and

---

[38] David Rowe, "Euclidean Geometry and Physical Space" (2006) 28:2 The Mathematical Intelligencer 51-59, 53.

[39] See for example, Ori Beklind, "Newton's Conceptual Argument for Absolute Space," (2007) 21:3 *International Studies in the Philosophy of Science* 271–293; Richard Westfall, *Isaac Newton* (Cambridge: Cambridge University Press, 2007).

[40] *Ibid*. Euclidean space is also known and become synonymous with Cartesian space referring to structural physical space: Nick Huggett, *Space From Zeno to Einstein: Classic Readings with a Contemporary Reading* (Cambridge, MA: MIT Press, 1999), but Cartesian originates with Rene Descartes: Rene Descartes, *The Geometry of Rene Descartes*, trans. By David E Smith & Marcia Lantham (New York: Dover Publications, 1954); for a detailed discussion on the evolution and development of scientific views of space, see Edward Grant, *Much Ado About Nothing: Theories of Space and Vacuum from the Middle Ages to the Scientific Revolution* (New York: Cambridge University Press, 1981).

[41] Hans Reichenbach, *The Philosophy of Space and Time*, trans by Maria Reichenbach (New York: Dover Publications, 1957).

[42] Huggett, *supra* note 40.

[43] Gottfried Leibniz cited in Brian Greene, *The Fabric of the Cosmos: Space, Time and the Texture of Reality* (New York: Vintage Books, 2004) 30.

[44] Geoffrey Martin, *All Possible Worlds: A History of Geographic Ideas*, 4th ed (New York: Oxford University Press, 2005); Nigel Thrift & Mike Crang, eds, *Thinking Space* (New York: Routledge, 2000); Leonard Guelke, *Historical Understandings in Geography: An Idealist Approach* (Cambridge, UK: Cambridge University Press, 1982).

place is the configuration in terms of physical positioning of objects in space. In this way, people and places are characterized in terms of a location on that grid and thus seen as "contingent features of a Euclidean set of spatial coordinates."[45] In this way, 'place' is marginalized because it refers to either a location somewhere or to the occupation of that location. For example, the first sense is of having an address and the second is about living at that address. The privileging of place as simply location has continued.[46] However, just as place and property are not the same thing, neither are location and place.

2.3 Location and Place

While the conceptual traditions suggest place and location are synonymous, points on the larger spatial grid, this dissertation supports maintaining a clear distinction between these concepts. In geographical terms, "location is the position of something, expressed in grid-coordinates, in relation to other things, or in such terms as near and far…. as the existence of fixed latitude and longitude coordinates on the

---

[45] Curry, *supra* note 17 at 258. Arrangements of objects on the face of the earth, characterized through the use of a mathematical system or grid is what mapping is all about. The current location-based technologies are built on mapping: Mark Monmonier, *Spying With Maps: Surveillance Technologies and the Future of Privacy* (Chicago, Ill: University of Chicago Press, 2002). This is exacerbated by the Google Maps view of the world where every place can be zoomed in and out from some space. Today, position determination and location-awareness, contemporary terms in the Euclidean tradition, are central to GPS enabled location-based services (LBS). LBS provide location-specific information for anyone with a GPS-equipped mobile device. This information can come in the form of advertisements, coupons, restaurant reviews, Wikipedia articles or information about the location of nearby services, such as gas stations or coffee shops. While these services do not necessarily reveal their users' locations to nearby people, users must allow the service provider to pinpoint their location to receive the desired local information: David Lyon et al, Location Technologies: Mobility, Surveillance and Privacy, Queen's University: The Surveillance Project (March 2005) at 6 online: The Surveillance Project <http://www.surveillanceproject.org/files/loctech.pdf>. As a subset of LBS, location-based social networks (LBSNs) transmit the users' location information to the service provider and share these locations with members of the users' social networks; Adrianna de Souza e Silva & Jason Firth, "Locative social mobile networks: Mapping communication and location in urban spaces" (2010) 5:4 Mobilities 485-505. Enhanced surveillance systems rely on context-aware technologies to observe and determine who, what and where. Space and location as characterized in physical geography reflect back into law, namely, in property law involving trespass (see for example, *Ontario Trespass to Property Act*, RSO 1990 c. T.21), territorial claims under section 8 of the *Charter* which "originally, legally and conceptually were tied to property." (*Dyment*, *supra* note 11 at para. 20); and in data protection laws of location information: *Personal Information Protection and Electronic Documents Act* SC 2000, c.5 [*PIPEDA*]; Teresa Scassa, "Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy" (2010) 7:2 CJLT 199-220.

[46] This appears to be a common refrain among geographers: see for example, John Agnew, "Space and Place" in John Agnew & David Livingston, eds, *Handbook of Geographical Knowledge* (London: Sage Publications, 2011) 316-330.

Earth's surface."[47] While places can also be located, they are not always stationary, as for example a cruise ship. Not all places have fixed geographical coordinates, as for example, 'cyberspace' might be considered a place, but it cannot be located. Heaven and Hell, as metaphorical spaces would likewise be considered as places but have no location. For Ginette Verstraete, "location refers to an abstract point in abstract space. As such it is devoid of meaning and cultural significance."[48] David Harvey corroborates by affirming that places have "a discursive/symbolic meaning beyond that of mere location, so that events that occur there have a particular significance."[49] Harvey is referring to the aspect of place he calls 'locale.'[50] For Harvey, since places almost always have a concrete form, 'locale' means the material setting, or actual shape of place within which people conduct their lives. For example, Ottawa is a collection of government buildings, shopping malls, churches and universities. A bedroom typically has four walls, a door, a window and a closet. Places then are material things, but even imaginary places, like the Emerald City have a physicality to them, such as rooms, hallways and stairs to the Wizard of Oz's domain. The point being, that a place is a geographical area encompassing physical or material settings with intrinsic qualities.[51]

Interestingly, however, with the increasing use of location-based services, location-aware devices and technologies, location acquires greater relevancy since

---

47 David Marshall Smith, *Moral Geographies: Ethics in a World of Difference* (Edinburg: Edinburg University Press, 2000).

48 Ginette Verstraete, *Mobilizing Place, Placing Mobility* (Amsterdam, Netherlands: Rodopi, 2002) at 12; see also John Agnew, *Place and Politics* (Boston, MA: Allen & Unwin, 1987); David Harvey, *Justice, Nature and the Geography of Difference* (Cambridge, MA: Blackwell, 1987).

49 Harvey*, ibid* at 293.

50 A 'locales framework' is featured in other work: see for example, Erving Goffman, *The Presentation of Self in Everyday Life* (Garden City, NY: Doubleday, 1959), which studies the idea of place as a setting for action and the ways in which behaviour depends on the social connotations of physical settings; the same idea is captured by Anthony Giddens, *The Constitution of Society: Outline of the Theory of Structuration*, (Berkeley, CA: University of California Press, 1984), 188: "[l]ocales refer to the use of space to provide the settings for interactions…[i]t is usually possible to designate locales in terms of their physical properties, either as features of the material world, or, more commonly, as combinations of those features and human artifacts." And while not expressly using the locales terminology, architect Malcolm McCullough adopts essentially the same approach: *Digital Ground*, *Architecture, Pervasive Computing, and Environmental Knowing,* (Cambridge, MA: MIT Press, 2005).

51 Doreen Massey, "The Conceptualization of Place" in Doreen Massey and Pat Jess, eds, *A Place in This World*: *Places, Cultures and Globalization* (Oxford: Open University Press, 1995) 45-77.

Influences and affects spatial interactions. For example, people check into locations, they are concerned about locational privacy, they have their location tracked, they attach information to locations, they socialize based on location and they are even able to create new locations.[52] Therefore, while distinct from place, when locations are combined with information, locations can also serve as mediators of spatial interactions. Viewed in this way, location has implications for privacy and surveillance, and the expectations we have in locations. What has been referred to as 'meaningful locations'[53] however creates a paradox; a personalized relationship to a physical location that at the same time may threaten and secure one's control of physical space.

In summary, although it appears that the ideas of 'space' and 'place' require each other for definition, this does not render them indistinguishable. And, it is an important distinction to make. Space is conceived of as an empty container, an infinite geometric expanse, a definition that is generally accepted today. On the other hand, when place is merely linked to location in that abstract space there is a lack of appreciation for its dynamic and experiential character. Ultimately, the concept of 'place' is seen largely as a common-sense idea. It seems clear what 'place' is not, but it is never actually defined nor developed as a distinct concept. Instead,"[s]ince Plato, Western philosophy – often times with the help of theology and physics – has enshrined space as the absolute, unlimited and universal, while banning place to the

---

[52] For example, *Foursquare*, a location-based social networking application, users can add new locations to the game, to which other users can check-in. A player can transform her bathroom into a new location and another player can become the mayor of his backyard if she defines it as a new *Foursquare* location. Or a person might define the spot where John Lennon was shot as a location and other visitors to New York will be able to contribute to the informational landscape of that location with comments, testimonies and pictures. Locations become filled with digital information that can be accessed, used and added to by others: <http://foursquare.com>; see also, "Wow! The foursquare community has over 10,000,000 members!" (June 20, 2011), online: Foursquare Blog <http://blog.foursquare.com/2011/06/20/holysmokes10millionpeople/>. See also Gregory Abowd et al, "Disclosure of Place: From Location Technology to Communication Practices" in Roy Want et al, eds, *Proceedings of the 3rd International Conference on Pervasive Computing* (London: Springer, 2005) 134-151; Daniel Sutko & Adrianna de Souza e Silva, "Location Aware Mobile Media and Urban Sociability" (2011) 13:5 New Media & Society 807-823.

[53] Harvey *supra* note 48.

realm of the particular, the limited, the local and the bound."[54] This fails to recognize the interactive nature of technology within a spatial environment and the role of people in the construction of places. The means by which places are constructed are far more complex than they had seemed when viewed simply as homogeneous settings. The phenomenological tradition of studying human experience in the world provides a more robust articulation of place.

3. People, Place and Lived Experience

Phenomenology provides a theoretical foundation that supplements abstract thinking about space with an understanding of the role of the body and the physical environment in human life.[55] As a philosophy, phenomenology is a particular way of approaching the world and apprehending lived experience.[56] The question of phenomenological inquiry is about the meaning of human experience, and asks: 'what is it like?' and then interprets the meaning of these experiences. Thus, phenomenological research "explores the humanness of being in the world."[57] The world, according to phenomenological perspectives, is a blend of human experience and physical structure. The way in which we act, the everyday, mundane, practical tasks and activities in which we are engaged and how they are accommodated into the world is what makes the world meaningful for us.[58] Its appeal is how it reorients the idea of space as a mere container and place as simply location to space as a setting for

---

[54] Arturo Escobar, "Culture Sits in Places" (2001) 20:2 Political Geography 139-174, 143.

[55] Herbert Spiegelberg, *The Phenomenological Movement* (The Hague: Martinus Nijhof, 1960); Christopher McCann, *Four Phenomenological Philosophers* (London: Routledge, 1993).

[56] Spiegelberg, *ibid* at 34.

[57] William Luijpen, *Phenomenology and Humanism* (Pittsburg, PA: Duquesne University Press, 1996); Jeff Malpas, *Heidegger's Topology: Being, Place, World* (Cambridge, MA: MIT Press, 2006).

[58] Edmund Husserl introduced the term 'life-world' to describe our everyday experiences in the world in "The Crisis of the European Sciences & Transcendental Phenomenology" (1936) cited in Peter Costello, *Layers of Husserl's Phenomenology,* (Toronto, ON: University of Toronto Press, 2012) 101-112. Similar to the Greek tradition where the words 'space' and 'place' did not exist, phenomenology's 'world' can be taken to mean the 'spaces' of our everyday lives: David Seamon, *A Geography of the Lifeworld* (New York: St. Martins, 1979); See also Michel de Certeau, *The Practice of Everyday Life*, translated by Steven Rendall (Berkeley, CA: University of California Press, 1984).

human activity and experiences. For anthropologist Marc Augé, effective enquiry concerning human activity can only take place if we stop considering space as a mere shell, a container, or a location, and start looking at it as a setting for action, experiences and communication.[59] The experiential nature of phenomenological theory emphasizes the embodied nature of human existence consistent with moving out off the screen into the physical world. It rejects the idea that we are entities detached from external reality, but rather sees us as subjects existing in the world, interacting with our physical environment. This resonates in the move from the disembodied nature of computing to the tangible and embodied interaction of ubicomp technologies in the real world.[60] The physicality of our bodies is linked with our experience of the physicality of our surroundings. Hence, this is a conceptual analysis well-suited for understanding spatiality, ubiquitous computing and ultimately, spatial privacy.

A central focus of phenomenology is the way people exist in relation to their world.[61] People do not exist apart from the world, but rather, are intimately caught up in and immersed in an "undissolvable unity" between people and world.[62] This is what Martin Heidegger called *Dasein*, which means everyday human existence or 'being-in-the-world.'[63] In other words, *Dasein* was the very essence of existence, the way humans exist in the world. He identifies the existential character of being-in-the-world with human beings propensity of inhabiting and dwelling. *Dasein's* way of being-in consists in dwelling or residing, that is, being 'alongside' the world as if it were at home there.[64] Heidegger holds that human beings and world are not two distinct entities, but only one which results from *Dasein's* involvement in the world. Thus, the 'in' of being-in-the-

---

59 Marc Augé, *Non-Places: An Anthropology of Supermodernity*, translated by John Howe (London, UK: Verso, 1995) 42-70; Joseph Kockelmans, *Phenomenology and Physical Science* (Pittsburg, PA: Duquesne University Press, 1966) 82-83;

60 See Chapter One, "Embodied Interaction" at p 48.

61 Martin Heidegger, *Being and Time*, translated by Joan Stambaugh (Albany, NY: State University of New York Press, 1996); Relph, *Place and Placelessness, supra* note 8.

62 David Stewart & Algis Mickunas, *Exploring Phenomenology: A Guide to the Field and its Literature* (Athens, Ohio: Ohio University Press, 1990) 9.

63 *Dasein* literal translation: "there" [Da] plus "being" [Sein], online: Wikipedia <http://en.wikipedia.org/wiki/Dasein>.

64 *Ibid* at 54.

world is unrelated to ideas of Aristotlean containment, instead 'in' is better understood in terms of involvement. For example, it is the 'in' of being in love, or in business, or being involved in the movie rather than sitting in row K. Heidegger therefore, characterizes everyday life as being an engaged, absorbed involvement in an undifferentiated world. A properly authentic existence to Heidegger is one rooted in place. If place is broadly analogous to this concept of dwelling, then to think of places as simply points on a map, or even as 'Toronto' or 'Paris' is a shallow conception of a place. Therefore, one significant dimension of the 'lifeworld' is the human experience of place.[65]

Our spatial meanings develop in no small part from the spatial nature of our bodies. The body is an anchoring point. Maurice Merleau-Ponty claims that our perceptions of space hinge on our capacity for action within it, based on the idea that we act with our bodies, which are already inherently spatial and located.[66] For Merleau-Ponty, "[s]pace is not the setting (real or logical) in which things are arranged, but the means whereby the position of things become possible."[67] We live and act in space. It is through action that we learn that places have structures and geometrical characteristics that can be schematized or mapped, and it is places that make the experience of space possible. We attach meanings and significance to space according to our body's capabilities within it. Place is thus embodied and practiced space, as opposed to the purely abstract notion of space as that which is unpracticed place.[68] It is, according to Edward Casey, "a striking fact, on which we do not often enough reflect,

---

[65] Edmund Husserl introduced the term 'life-world' to describe our everyday experiences in the world. Similar to the Greek tradition where the words 'space' and 'place' did not exist, phenomenology's 'world' can be taken to mean the 'spaces' of our everyday lives. David Seamon, *A Geography of the Lifeworld* (New York: St. Martins, 1979); See also Michel de Certeau, *The Practice of Everyday Life*, (Berkeley, CA: University of California Press, 1984); similarly, philosophers argue for a much more fundamental role of place in life. Casey, *Getting Back into Place*, *supra* note 15 at 15-16, argues that 'place' is a central ontological structure founding human experience: "place serves as the condition of all existing things…[t]o be is to be in place." Malpas, *Place and Experience*, *supra* note 15 at 35, claims "place is primary to the construction of meaning and society. Place is primary because it is the experiential fact of our existence."

[66] Maurice Merleau-Ponty, *The Phenomenology of Perception*, trans by Colin Smith (New York: Routledge, 1958/2003).

[67] *Ibid* at 284.

[68] Casey, *Getting Back Into Place, supra* note 15 at xv.

that while we can certainly *conceive* of entirely empty spaces and times – radical vacua in which no bodies (in space) or events (in time) exist – such spatial-temporal voids are themselves placelike insofar as they *could be*, in principle, occupied by bodies and events."[69]

These phenomenological theories are not only important, but essential to the ways we conceive of embodiment and place as we move closer to a ubiquitous computing environment. We may think of space as abstract and non-physical, but lived space is physical. We cannot escape spatiality. We are spatial beings, we live and interact in space. Real space is always inhabited and situated, becoming place.[70] Tangible, or spatial, interaction is embedded in real space and the interfaces are situated in places. Phenomenological analysis provides the basis for a richer understanding of place in the real world.

3.1 Place

Informed by phenomenology, popularized discourse on the notion of 'place' began in the 1960's in the area of urban planning.[71] Jane Jacobs argued that in planning, one needs to look at the people who live and work in urban neighbourhoods and view these neighbourhoods not simply as districts or regions, but rather as places constructed through everyday activities. This approach changed the direction of urban planning in which designers were not just concerned with three-dimensional structures, but also with the places for people to be.[72] It became generally accepted that the focus on buildings did not take into account "that all the life and soul of a place, all of our experiences there, depend not simply on the physical environment, but on the pattern of events which are experienced there."[73] Thus, the close relationship between people and their environment and the ways in which people use spaces, and interact

---

[69] *Ibid* at 13.

[70] Stephen Harrison and Paul Dourish, "Re-place-ing Space: The Roles of Space and Place in Collaborative Systems" in *Proceedings of CSCW* (New York: ACM Press, 1996) 67-76.

[71] Jane Jacobs, *The Death and Life of Great American Cities* (New York: Vintage Books, 1992); as cited in Curry," Discursive Displacement"*, supra* note 17.

[72] Christopher Alexander, *The Timeless Way of Building* (Oxford, UK: Oxford University Press, 1979).

[73] *Ibid* at 62.

within places. Anthropologist Edward T. Hall's work pointed to the ways in which people interact with one another within places.[74] Many of the ideas originating with Jacobs and Hall moved, in part, into the social sciences where it became formalized in environmental psychology.[75]

While early work within environmental psychology, studying the relationship between humans and their surroundings, did not conceptually distinguish between space and place, more recent work in this field focuses on 'place' as a concept capturing people's relationships with the physical environment in which they act, the lived experience of place.[76] David Cantor points out that our presence in the environment is purposeful because we actively modify, build and influence our physical surroundings, rather than simply react to a certain environmental layout, or to particular variables.[77] In his view, the experience of place is grounded in the physical characteristics of the environment, and interaction with it, but also is bound up with the individual's previous experience and expectations.[78] In this way, it is a step away from the vision of space as purely a structure and towards the consideration of its qualities of use and of its dynamic nature, while still acknowledging the significance of physicality. Similarly, Lynne Manzo enlarges the conception of place by addressing the nature of our interactions with and in physical space. For Manzo, place meaning depends on the

---

74 Hall, *The Silent Languag*e, *supra* note 23.

75 Environmental Psychology as it relates to spatial theory expressed concern not simply with physical space, but with the connections between human behaviour and physical surroundings in order to understand the way people interact in and with the environment. While 'place' is grounded in the physical characteristics of the environment, and interaction with it, it also takes its meaning from the individual's expectations of the place. Robert Sommer, *Personal Space*, *supra* note 23; Julian Edney, "Human Territoriality", *supra* note 22; Irwin Altman, *The Environment and Social Behaviour: Privacy, Personal Space, Territory and Crowding* (Monterey, CA: Brooks/Cole, 1975); Harold Proshansky, *Environmental Psychology: People and his Physical Setting* (Austin, TX: Holt Rinehart, 1976); Robert Gifford, *Environmental Psychology: Principles and Practice* (Coleville, WA: Optimal Books, 2007).

76 David Canter, "The Facets of Place" in Gary T Moore & Robert W Marans, eds, *Advances in Environment, Behaviour and Design* (New York: Plenum, 1997) at 109-148; Per Gustafson "Meanings of Place: Everyday Experience and Theoretical Conceptualizations" (2001) 21:1 Journal of Environmental Psychology 5-16; Bradley Jorgensen & Richard Stedman, "Sense of Place as an Attitude" (2001) 21 Journal of Environmental Psychology 233-248; Lynn Manzo, "Beyond House and Haven: Toward a Revision of Emotional Relationships with Places" (2003) 23:1 Journal Environ. Psychol. 47-61 and "For Better or Worse: Exploring Multiple Dimensions of Place Meaning" (2005) 25:1 J Environ. Psychol. 67-86.

77 Cantor, *ibid* at 112.

78 *Ibid* at 117.

experiences we live in those places; the *experiences-in-place*.[79] It is through the experiences that we consider relevant and important to us, that we form significant relationships to places. Hence, the places themselves are not important. The experiences that are lived in the places make them important.[80] Places become significant because they afford opportunities for privacy, introspection and self-reflection.[81]

3.2 (Re)Discovering Place in Geography

Place and geography are important theoretical orientations in this dissertation. Indeed, to discuss place is to discuss a quintessence of geography. Territorial privacy, as discussed in Chapter Three, is one of the zones of constitutional privacy protection that has been legally and conceptually tied to places, or people *in* physicalized private places. The law rests on a particular notion of place narrowly interpreted as a fixed geographic location in abstract space, and on traditional views of what is private and what is public. Neighbourhoods, towns, cities, or a home are more easily thought of as places, but on a smaller scale, so too can a corner of a room in your home or a favourite park bench on the river be places. Yi-Fu Tuan suggests there is something of place in all of these, so places-as-things is difficult to grasp.[82] Where you are is important, increasingly so in the ubiquitous computing context, but location alone ought not be determinative.

Humanistic geography, a branch of geography which studies how humans interact with their spatial environments,[83] brings the concept of 'place' explicitly to the forefront of geographical enquiry seeking to formulate a more subjective and experiential account of place.[84] For humanists, 'space' is seen as an abstract

---

79 Manzo, "For Better or Worse" *supra* note 76.

80 *Ibid* at 70.

81 *Ibid* at 76.

82 Yi-Fu Tuan, "Space and Place: Humanistic Perspective" (1974) 6 Progress in Human Geography 211-252.

83 Erin Fouberg & Alexander Murphy, *Human Geography: People, Place and Culture* (Hoboken, NJ: Wiley & Sons, 2009).

84 Tuan, *supra* note 82; Relph, *supra* note 8; Robert D Sack, *Homo Geographicus* (Baltimore, MD: John Hopkins University Press, 1997); Mike Crang & Nigel Thrift, *Thinking Space* (London: Routledge, 2000);

geometrical extension and location whereas 'place' describes our experience of being in the world and investing a physical setting with meaning. Humanistic geography "looks at the environment and sees place, that is, a series of locales in which people find themselves, live, have experiences, interpret, understand, and find meaning."[85] It seeks to move beyond traditional geography's strict association of place with the physical characteristics of locations and their empirical categorization. Space is the physical world, the objects, artifacts, air and the like that make up the world of space, the three-dimensional extended world of reality as it is presented to us. Place, on the other hand, is space which has meaning, a particular geographic location which has meaningful attachments to the people who pass through it. Seen in this way, places exist on top of spaces in that physically, a place is a space invested with understandings of behavioural appropriateness and expectations. We are located in 'space' but we act in 'place.' Spaces then, can become places, not just a physical 'container' for individuals and their tasks, but a setting where complex interactions occur. For humanists, place is seen as not just a thing in the world, but a way of understanding the world.[86] How, then, does human geography conceptualize 'place'?

Yi-Fu Tuan uses the term 'topophilia' to refer to the "affective bond between people and place."[87] This bond, this sense of attachment, is fundamental to the idea of place as a "field of care."[88] He defines place through a comparison with space: "If we think about space as that which allows movement, then place is pause, each pause in movement makes it possible for location to be transformed into place."[89] He develops then a sense of space as an open arena of action and movement while place is about stopping, resting and becoming involved. This kind of discussion of place is clearly much more than a discussion of location or region. Because place is a product of a

---

Anne Buttimer, "Grasping the Dynamism of Lifeworld" (1976) 66:2 Annals of the American Geographers 277-292.

85 Richard Peet, *Modern Geographical Thought* (Oxford: Blackwell, 1998) 48.

86 Cresswell, *Geographic Thought*, *supra* note 33; Curry," Discursive Displacement*", supra* note 17

87 Tuan, *supra* note 82 at 4.

88 *Ibid*.

89 *Ibid* at 6.

pause and a chance of attachment, it exists at many scales: at one extreme a favourite armchair is a place, at the other extreme the whole earth:

> Place can be as small as the corner of a room or as large as the earth itself. That the earth is our place in the universe is a simple fact of observation to homesick astronauts…It is obvious that most definitions of place are quite arbitrary. Geographers tend to think of place as having the size of a settlement, the plaza within it may be counted a place, but usually not the individual houses, and certainly not that old rocking chair by the fireplace.[90]

The implication here is that the abstractions of spatial science simply miss out too much of the richness of human experience. Places are experienced and could not be measured or mapped. What begins as "undifferentiated space becomes place as we endow it with value and invest it with meaning."[91]

If that is 'what' place is, how does meaning become associated with places? The essential quality of place was its power to order and to focus human intentions, experience and behaviour spatially. Relph identifies "physical appearance, activities and meanings" as what he called the "raw materials" of the identity of places.[92] Physical appearance means the structure, layout and perceivable qualities of a setting; activities encompass social activities, economic functions and routines; and meanings refer to the particular significance deriving from past events and present situations, rooted in the physical settings but a property of human intentions and experiences. These three fundamental components are "irreducible one to the other, yet are inseparably interwoven in our experiences of place."[93] In other words, to truly understand the essence of place, these materials cannot be considered individually, in isolation from one another. Instead, the identity of place is created by the interconnections between them.

---

[90] Tuan, *ibid* at 245.

[91] Tuan *ibid* at 82. Similarly, Relph, *supra* note 8 at 8, compares space with place to illustrate the significance of place to human life: "[s]pace is amorphous and intangible and not an entity that can be directly described and analyzed. Yet, however, when we feel or explain space, there is nearly always some associated sense or concept of place. In general it seems that space provided the context for places but derives its meaning from particular places."

[92] Relph, *ibid* at 47-48.

[93] Relph, *ibid*.

For Tuan, place exists only as it is made by people's experience. There are certain elements that constitute this experiential place. It is grounded in the material reality of the world in which we make places of spaces we can physically sense, explore and inhabit. The physical element expresses how characteristics can manifest a sense of place.[94] It can take different forms, from objects within a home, to urban architecture, to geographical locations such as a neighbourhood or city. The feelings, emotions, memories, knowledge and background we associate with a place invest it with meaning within those places. In other words, the subjective element describes how personal sensing and emotions are related to place. The person's experience and identity influence the subjective sense of place[95] and induce attitudes and behaviours within those places.[96] Place-feelings may contribute to the formation, maintenance and preservation of the identity in which a place becomes a symbol for self.[97] Social interaction and communication within the place contribute to the experience of place. The social element explains how others and people's social behaviour form how people relate to place.[98] As well, there are cultural rules, conventions and identity of a place which influence an understanding beyond its built or material character. Therefore, in the activities people perform, spaces are experienced and lived through these overlapping yet distinct elements and are made into places. Place is understood as a 'lived space' which is irreducible to physicality alone. It transcends its structural dimensions to encompass human activity as constituent of the identity of the space

---

94 James Duncan, "Place" in Ron Johnston et al, eds, *The Dictionary of Human Geography* (Oxford, UK: Blackwell, 2000); Richard Stedman, "Is it really a social construction? The contribution of the physical environment to sense of place" (2003) 16:8 Society & Natural Resources 671-685.

95 Massey, *supra* note 51.

96 Mae Davenport & Dorothy Anderson, "Getting from sense of place to place-based management: An interpretive investigation of place meanings and perceptions of landscape change" (2005) 18:7 Society & Natural Resources 625-641.

97 Altman & Low *supra* note 8.

98 Robert Hay, "Sense of Place in Development Context" (1998) 18:1 Journal of Environmental Psychology 5-29; Nicholas Entrikin, *The Betweenness of Place: Towards a Geography of Modernity* (Baltimore, MD: John Hopkins University Press, 1991); see also Henri Lefevre, *The Production of Space* (Oxford: Blackwell, 1991). Although socially produced space is often confused with experiential place, in many ways, social space plays the same role: Cresswell, *supra* note 33 at 122-146.

itself.[99] The combination and interplay of these elements is, effectively, 'place' as contextual.[100] To look for a causal relationship between these elements is to reduce the 'contextual' nature of place meaning and will fail to capture the "personality" of place.[101]

3.2.1 No Place Like Home

For many**,** the most familiar example of place and its significance to people is the idea of the home. For Tuan, home is an exemplary kind of place where people feel a sense of attachment and rootedness and, more than anywhere else, is seen as a center of meaning and a field of care.[102] Home, for many, is an intimate place of rest where a person can withdraw from the hustle of the world outside and have some degree of control over what happens within a limited space.[103] The centrality of home to humanistic approaches to place owes much to Heidegger's focus on 'dwelling' as the ideal kind of authentic existence[104] and to the work of Gaston Bachelard.[105] Bachelard considers the home as a primal space that acts as a first world or first universe that then frames our understandings of all spaces outside. The home is an intimate space

---

[99] Merleau-Ponty, *Phenomenology of Perception*, *supra* note 66.

[100] See for example, Fritz Steele, *The Sense of Place* (Boston: CBI, 1981) at 11-12; Jorgensen & Stedman, *supra* note 76 at 671; and Cresswell, *supra* note 33 at 139, all supporting a contextual analysis to the complex creation of place meaning. Ultimately, each approach identifies the same elements, albeit with different terminology and with some variability of emphasis. Common to these approaches, however, is a belief that reduction of the experience into component parts fails to capture the fullness of the human place experience. It is the summation of the interactions and connections that place is expressed. All aspects combine to create place meaning and it is not feasible to specify the degree of influence exerted by each component, which may, in fact, vary by situation.

[101] Trevor Barnes & Michael Curry, "Towards a Contextualist Approach to Geographical Knowledge" (1983) 8:4 Transactions of the Institute of British Geographers 467, 472.

[102] Yi-Fu Tuan, "A View of Geography" (1991) 81:1 Geographical Review 99, 101; for critique of this idea of home, see Gillian Rose, *Feminism and Geography: The Limits of Geographical Knowledge* (Cambridge: Polity, 1993) 43.

[103] David Seamon, *A Geography of the Lifeworld, supra* note 58; This idea of home as a fundamental place has been questioned by feminist geographers. See for example, Gillian Rose, *Feminism and Geography: The Limits of Geographical Knowledge* (Cambridge: Polity, 1993); Bell Hooks, "Homeplace: a site of resistance" in Bell Hooks, *Yearning: Race, Gender, and Cultural Politics* (Boston: South End Press, 1991); Iris Marion Young, "House and Home: Feminist variations on a theme" in Iris Marion Young, *Intersecting Voices: Dilemmas of gender, political philosophy, and policy* (Princeton, NJ: Princeton University Press, 1997).

[104] Martin Heidegger, "Building, Dwelling and Thinking" in Heidegger, *Poetry, Language and Thought*, trans by Albert Hofstadter, (New York: Harper Colophon Books, 1971).

[105] Gaston Bachelard, *The Poetics of Space: The Classic Look at How We Experience Intimate Places*, translated by Maria Jolas (New York: Orion Press, 1964).

where experience is particularly intense.[106] For Bachelard, then, the home is a particularly privileged kind of place that frames the way people go on to think about the wider universe.

This privileging of the home is historically reflected in law. From the origins of the common law, the home has been a presumptively private place. As Sir Edward Coke famously held, "the house of everyone is to him as his castle and fortress."[107] Connoting personal autonomy, privacy and retreat, the home is understood as a singular kind of place, continuing to serve as a key locus for distinguishing between the public and the private. The Supreme Court of Canada continues to acknowledge the home as a presumptively private place, although where there has been no physical trespass or when an informational analysis is employed, the reasonable expectations of spatial privacy involving the home are potentially eroded.[108]

3.2.2 Place and Ubiquitous Computing

Hybridization is a characteristic of technology-infused lived spaces.[109] Embedded computational technologies mix the real and virtual worlds, highlighting the concept of place as hybrid. Adrianna de Souza e Silva characterizes hybrid spaces as emerging from the use of mobile devices.[110] For de Souza e Silva, because "mobile devices create a more dynamic relationship to the Internet, embedding it in outdoors everyday activities, we can no longer address the disconnection between physical and digital spaces."[111] Thus, the virtual is not the opposite of the real, but instead a component of experiencing the real. The virtual serves as a way to understand the real.

---

[106] The 'smart home' augments people's lives with ubiquitous computing, providing increased communication, awareness and functionality. While this technological embeddedness does not necessarily change the sense of place one feels or associates with the home, it does alter it. People now live in "glocality" defined as being inside and outside at the same time: Joshua Meyrowitz, "The Rise of 'Glocality" in Kristof Nyiri, ed, *A Sense of Place* (Vienna: Passagen Verlag, 2005) 21-30 The home remains a physical place of attachment, but our experiences of home are no longer purely local and we are less likely to see our physical surroundings as the source of all experiences.

[107] *Semanynes*' Case, 77 Eng. Rep 194, 195, 5 Co. Rep. 91a, 91b (K.B. 1604).

[108] See for example, *Tessling*, *supra* note 5; *Gomboc*, *supra* note 5; and to some extent, *Patrick*, *supra* note 5.

[109] See Chapter One, "Hybridization" at p 40.

[110] Adriana de Souza e Silva, "From Cyber to Hyber: Mobile Technologies as Interfaces of Hybrid Spaces" (2006) 9:3 Space & Culture 261-278.

[111] *Ibid* at 263.

For example, in terms of our embodied engagement with mobile devices, which simultaneously occurs in our everyday places, the real and the virtual cannot be used in isolation from one another. What takes place across the virtual space of mobile computing is founded on the interaction in the real, or material, world.[112] Our sense of self can be developed from interactions that take occur across geographically distant places and in terms of intimate interpersonal connections, face-to-face is now implicated and informed by the virtual.[113]

When viewed from the humanistic geography lens, a hybrid place experience does not denote a single place, but instead is an experience being distributed over many places. In other words, a hybrid place experience is distributed over virtual and physical environments. In this way, a place experience is not necessarily tied to a certain location and similarly, a certain location is not necessary to place making. Ubiquitous computing technologies extend the possibilities to experience places without having to move in and out of the actual geographic place. This is an important point in the context of spatial privacy in law because, as described in Chapter Two, modes of surveillance continue to move into digital forms in and out of physically private places. The adherence to traditional distinctions between private and public become less useful to accurately describe our experiences with embodied places.

4. Conclusion

Ubicomp is not simply about computing but also about the relationship between that computation capacity and the world in which it resides. What makes Weiser's model unusual is that it is not just about faster processors and algorithmic advances, but about a new kind of computing. Computing that is woven into the fabric of everyday life. In other words, a new place, or lived spaces for computing. What place is and where this place will be found is significant. Available beyond the desktop, carried

---

[112] See Chapter One.

[113] Soraj Hongladarom, "Pervasive Computing, Privacy and Distribution of the Self" (2011) 2:2 Information 360-371.

with us, encountered as embedded in the built environment, and operating in augmented artifacts we interact with. Place, then, should be seen as less about an absolute location, a spot on the map, and more about connections with the many sites in our lives. Grounding life in effective contexts remains absolutely necessary, but this means a conception of place that encompasses all the dimensions of our lived experiences. Moreover, although the concept of place is complex, we need to be concerned with the predominant discourse on data protection because this focus, in the process, fails to see the role and meaning of places in everyday life. The application of the data-protection approach, and narrow interpretation by the Supreme Court of personal information, fails to take into account the importance of everyday activity, and the damage that results to people *and* places in not safeguarding lived spaces.

Place is not just the 'where' of something. It is the location plus everything that gives that location meaning. It is a process involving complex integrations that continue to develop and which connect flows of people[114] and the "space of places."[115] In any given place we encounter a combination of physicality *and* meaning. The experiential conception of place, as developed within phenomenology, environmental psychology and particularly, humanistic geography, better reflects this spatiality and interactive nature of our everyday lives. Based on these foundations, a new conceptual construct of 'peopled places' is proposed in Chapter Five, seeking to overcome the extent to which law is currently constrained by its reliance on traditional geography and property concepts. Chapter Five develops the peopled places construct around four defining features: embodiment, contextual dimensions, mobile interactions and boundary management. Having built an alternative conceptual apparatus, Chapter Five provides legal examples that illustrate how the peopled places construct will better accommodate privacy interests in an environment of ubiquitous computing.

---

[114] F Lukerman, "The Geography of Utopia" in David Lowenthal, ed, *Geographies of the Mind*, (New York: Oxford University Press, 1976) 226-249.

[115] Manuel Castells, "Space of Flows, Space of Places: Materials for a Theory of Urbanism in the Information Age" in Tigran Haas, ed, *New Urbanism and Beyond: Designing Cities for the Future* (New York: Rizzoli, 2008) 314-321.

CHAPTER FIVE

PEOPLED PLACES: FROM TERRITORIAL TO SPATIAL PRIVACY

Man and his extensions constitute one interrelated system.

Edward T. Hall, *The Hidden Dimension* (1969)

1. Introduction

In 1921, Ludwig Wittgenstein published *Tractatus Logico-Philosophicus*, a dense, complex work seeking to explore the nature of facts.[1] Wittgenstein discusses a "picture theory" of meaning, according to which language represents, or pictures, the relationships between entities in the world. He argued that language could be seen as picturing the world so that a linguistic statement had the same logical structure as some states of affairs in the world, claiming "[t]he limits of my language mean the limits of my world."[2] However, Wittgenstein later takes the position that he had relied on a set of spatial terms that were in fact merely metaphorical.[3] In the end, he no

---

1 Ludwig Wittgenstein, *Tractatus Logico-Philosophicus*, trans by DF Pears & BF McGuinnes, 1961 (London: Routledge 1921).

2 *Ibid* at 5:62. See also, Rich Gold, "This is Not a Pipe" (1993) 36:7 Communications of the Association of Computing Machinery (ACM) 72. As cited in the article, the title 'This is Not a Pipe' is based on a painting, reproduced with the article, by French surrealist artist Rene Magritte of a pipe with the caption 'Ceci n'est pas une pipe.' For Gold, reproductions, resemblances or digitally-enabled images of real things blanket the world, but these are images or representations only. The pipe is not a pipe and the painting of the pipe is just that, "a replica." What Gold calls the skin of an object, like language, replicates meaning and content. It does not replicate what we actually associate with the object in the real world because "the image of an object is not the same as its Real McCoy, 3D cousin." The pipe, or the everyday coffee maker may look the same, but they do not act the same. The everyday objects themselves become a kind of a "ruse." A toy doll "might look like a familiar remnant of childhood, but it is really only of of a thousand distributed nodes which control the functioning of the whole house…and likewise, itself activates its own mechanisims." In this way, Gold describes the next phase of computing not in terms of its technical frameworks, but as a new way of seeing and engaging with the world.

3 Ludwig Wittgenstein, *Philosophical Investigations*, trans by GEM Anscombe, 1968 (Oxford: Blackwell, 1953).

longer held the view that words simply signify states of the world because they are very often simply images that turned attention away from the fact that words only have meanings within the contexts of the individuals that use them in particular situations and particular places. Similarly, this dissertation calls into question a view of the world where people are seen merely as objects in which the map and informational images are capable of capturing the spatiality of our everyday lives. A view persistently reinforced by privacy jurisprudence as a result of being stuck in the language and meaning of 'place' as bounded and defined geographical territory. Hence, the description of the spatial dimension of privacy as the 'territorial' zone.

This needs to change. We must consider an alternative conception of place because "the most profound technologies are those that disappear [and] weave themselves into the fabric of everyday life"[4] transcending physical territoriality. For all the advantages, conveniences and safety that ubiquitous computing can potentially provide, the surveillance practices it facilitates more directly and more pervasively implicate spatial privacy interests. To move privacy law beyond narrow interpretations and naive perceptions of place, Chapter Four began this process by outlining theories of space and place, adopting the experiential conception of place because it best reflects the spatiality central to our everyday lives and expectations in the real world. It understands place not just as a location, but emphasizes the experiences of place and human-place interactions, an approach concerned with the way we experience the world; through and in place. For Yi-Fu Tuan, "[p]lace incarnates the experiences and aspirations of people. Place is not only a fact to be explained in the broader frame of space, but it is also a reality to be clarified and understood from the perspectives of the people who have given it meaning."[5]

Chapter Five builds on these ideas to develop an alternative construction of place to inform and shape, and be shaped by, privacy law. This Chapter proposes a conceptual construct of 'peopled places' that transcends bounded territory and gives

---

[4] Mark Weiser, "The Computer for the 21st Century" (1991) 265:3 Scientific American 66.

[5] Yi-Fu Tuan, *Space & Place: The Perspective of Experience* (Minneapolis: University of Minnesota Press, 1977) 387.

effect to people *and* places. Characterized in this way, place is embodied and contextual, grounded in the practices of everyday life. Constructing 'peopled places' is based on how people experience place and what makes places meaningful, encompassing four defining features set out in this chapter. First, place begins with *embodiment* because it is practically impossible to think of places outside the body. Everything we do, we do with our bodies. When we think, speak, listen, eat, sleep, walk, relax, work and play we 'use' our bodies. Every aspect of our lives is therefore embodied. The body as it is performed in everyday life is realized through its interactions with its environment, an environment materially and spatially mediated. When we experience a place, we do so through our body, which acts as a layer between a place and our perception of it. Second, place is experienced by people along different, although dynamically interconnected *contextual dimensions*. Our daily lives are lived through physical, personal, social and cultural contexts where human activities make sense and where they derive their meaning. Third, 'every*ware*' computing is characterized by complex *mobile interactions* and interconnections between information and communication technologies in the real world. Thus, the way in which we experience the places in which we live transforms how we relate and engage with those places. And finally, the issue of *boundaries* presents perhaps the greatest challenge for thinking about place in productive ways, compounded by the blurring of boundaries in a ubicomp environment, yet at the same time a legal framework that continues to invoke the private-public analysis. Having developed an alternative construction of place in Part One of this Chapter, how can it be applied in privacy law? Part Two of this chapter will give examples of current approaches and show how the peopled places construct will better accommodate privacy interests in an environment of pervasive computing.

2. The Construct of Peopled Places: Four Defining Features

2.1. The Embodiment of Place

Although it is possible to think of the body as flesh surrounded by skin, this account of the body-as-container is too simple. We are spatial beings; our bodies are a central reference point for characterizing lived spaces, or place. The lived experience of the body mediates between the self, identity and the world we encounter.[6] Yet, strangely, the body's engagement with and in the material world is neglected in privacy jurisprudence, confounded by purporting to protect 'people not places.'[7] Moreover, embodiment does not simply mean physical manifestation. Rather, it means being grounded in and emerging out of everyday, mundane experience. Perhaps, as Julie Cohen suggests:

> We should understand the persistent recurrence of privacy concerns around bodies and spaces as telling us something important about the nature of privacy and privacy invasion as experienced…the relation between self and society is not, and never has been, a purely informational one, but rather is materially and spatially mediated. Privacy law and theory need to recognize the importance of bodies and spaces before the account of privacy interests can be complete.[8]

This is rendered more pressing as ubiquitous computing integrates our embodiment with the environment and objects within that environment.

Embodiment is rooted in the ways in which people participate in the world.[9] It is about interaction and how we act in a world that is filled with meaning, which both makes our activities meaningful and is itself transformed by them. In the context of 'every*ware*', tangible embodiment factors in to the construct of peopled places because it is characterized by tangible computing, or physicality with the real world.[10] Tangible

---

6 Martin Heidegger, *Being and Time*, trans by Joan Stambaugh (Albany, NY: State University of New York Press, 1996); Merleau-Ponty, *The Phenomenology of Perception*, translated by Colin Smith (New York: Routledge Press, 1958).

7 See Chapter Three.

8 Julie Cohen, *Configuring the Networked Self: Law, Code and the Play of Everyday Practice* (New Haven, CT: Yale University Press, 2012) 15.

9 See Chapter Four, Section 3: 'People, Place and Lived Experience' at p 156.

10 See Chapter One, "Physicality" at p 30 and "Embodied Interaction" at p 44.

computing, unlike 'desktop computing' draws on embodiment by recognizing the physical embedding of action in the world.[11] In other words, ubicomp blends computation and physicality thereby extending interaction into the real world. Augmented physicality takes us away from the desktop to other ways of interacting. Tangible computing incorporates information provided by the computer into the user's physical environment and physical interactions. In short, 'bits' become embodied. The 'here and now' describes the immediate, embodied presence of an object or place. For example, location-aware technologies such as GPS-enabled cell phones bring place to the forefront of users' embodied interaction with information, the physical environment and other users. In other words, the body is brought to the forefront as the essential and defining site of interaction and experience.

Devices proximate to the body, or distributed in the physical environment, are able to read, measure, track and provide feedback on our location, proximity, gestures, movement, breathing, pulse, emotional state and gaze. What we carry or wear and how we move through lived spaces in our daily interactions influence our experiences of the world around us and our agency to act in our everyday lives. By capitalizing on the contextual features of presence, location and activity, it unifies the physical and digital worlds to create a blend, which more closely matches our daily experiences, tasks and activities. However, in the context of surveillance, this blending lends itself to the body being reduced to a digital representation and effectively the disappearance of the physical human body, the very source and space of surveillance. While digital and physical observation may be informationally equivalent, they are not interactionally equivalent. When digital, or electronic, representations are uncoupled from the physical person, the observed become perceived in a disembodied way. The body is left behind, replaced or translated into a digital abstraction or representation, which fails to take into account the embodied interaction by which it occurs. Hence, the focus is on a data construct[12] rather than on the lived spaces people make meaningful through embodied interaction. The peopled places construct extends beyond simply an

---

[11] *Ibid.*

[12] Daniel Solove, *The Digital Person: Technology and Privacy in the Information Age* (NY: NY Press, 2004).

awareness of spatial location, of user identity and of proximity of people and devices to encompass the interactive bodily experiences, which contribute to shaping our sense of self and identity. Once we better understand places as "peopled", we can recognize the need to rethink the territorial construct as a legal means to protect privacy. Although a body may not be physically present during the manipulation of an embedded environment, in an ubicomp context, such a "search" may implicate the person without them physically 'being there.'

2.2 Contextual Dimensions of Peopled Places

Since *R v Edwards,* the Supreme Court of Canada's standard methodology for assessing whether a *Charter* claimant has a reasonable expectation of territorial privacy is determined by the "totality of circumstances." [13] The circumstances include "presence at the time of the search; possession or control of the property or place searched; ownership of the property or place; historical use of the property or item; and the ability to regulate access."[14] This set of circumstances does provide a contextual framework for analyzing reasonable expectations of privacy but, once unpacked, ones sees that it still essentially relies on the zonal classification scheme for assessing privacy claims, further entrenching territorial privacy in the traditional private-public distinction. Moreover, the *Edwards* contextual analysis may not go so far as to explicitly convert section 8 into a property right, nor is the place searched

---

13 *R v Edwards,* [1996] 1 SCR 128 at para 31 [*Edwards*].

14 *Ibid*. See also, for example, *R v Ritter*, 2006 ABPC 162, 402 AR 249 (no reasonable expectation of privacy in a rented storage unit); *R v Simpson*, [2005] OJ No 5056 (QL) (ON Sup Ct Jus) (no reasonable expectation of privacy in apartment building's hallway since the accused did not own the hallway and he could not regulate access to it); *R v Osanyinlusi*, [2006] OJ No 2529 (QL) (ON Sup Ct Jus) (no reasonable expectation of privacy in the bedroom where accused lived because the door was left open, no efforts were made to exclude others from the room and the accused did not control access to its contents); *R v Belnavis*, [1997] 3 SCR 341 [*Belnavis*] (a passenger in a car has no reasonable expectation of privacy).

Note Binnie, J. in *R* v *Tessling,* [2004] 3 SCR 432 at para 32 [*Tessling*], applies the *Edwards* framework but modifies to fit an informational privacy analysis where there is no physical intrusion. This version of the "totality of circumstances" includes "whether the subject matter was in public view; whether the subject matter had been abandoned; whether the information was disclosed to third parties; and whether the information gathered exposed any intimate details of lifestyle or information of a biographical nature. See also, for example, *R v Gomboc*, [2010] 3 SCR 211 [*Gomboc*].

determinative, its emphasis is on proprietary interests.[15] In other words, the spatial context being considered is far too narrow. The construct of 'peopled places' offered in this dissertation provides a richer context for what counts as place, an account that is essential for the possibility of preserving privacy in a ubicomp environment.

The conception of peopled places is grounded in a vision of place as experiential, that is, people and their experience of a setting create and shape the meaning of place. At the same time, place can only be grounded in the physical, material reality of the world. We make places of spaces through physically sensing, exploring, inhabiting and interacting with them. Thus, the first dimension of peopled places is the physical context, but defined more broadly than it is currently conceived. Consequently, the peopled places construct need not diminish the protection afforded the home, and in many instances expands it. In addition to the physical aspect, the social dimension, or context, contributes to the experience of making place. Although related, the social context of peopled places used here is not referring to the shared or common social good of privacy,[16] but rather the contexts in which social and technological interactions occur. Each of these dimensions, the physical and the social, is present at any moment of one's experience of a place and the experience is shaped by the dynamic interconnections of these dimensions. The contexts should not be seen to exist *a priori*, as a series of abstract categories but, rather, emerge through people's actions, activities, practice, interactions and experience. In other words, a place is a chain-link of people connected through a set of contingent features. The place itself may simply be seen as a spatial location, but the relationship between people and places is far richer and more complex than that. Peopled places capture this complexity

---

[15] It is also contrary to the liberal and purposive approach articulated in *Hunter v Southam Inc*, [1984] 2 SCR 145 [*Hunter*]; and reminiscent of the risk analysis that the Supreme Court of Canada rejected in both *R v Duarte*, [1990] 1 SCR 30 [*Duarte*] and *R v Wong* [1990] 3 SCR 36 [*Wong*].

[16] See for example, Priscilla Regan, *Legislating Privacy* (Chapel Hill: University of North Carolina Press, 1995); Alan Westin, "Social and Political Dimensions of Privacy" 59:2 2003 J. of Social Issues 431-453; Valerie Steeves, "Reclaiming the Social Value of Privacy" in Ian Kerr, Valerie Steeves & Carole Lucock, eds, *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked* Society (Toronto, ON: Oxford University Press, 2009) at 191.

by acknowledging important aspects of our personal and practical lives; taking into account both the broader physical context and the social context.

The Broader Physical Context

A central theme of this dissertation is that if privacy is to protect people, it must protect them in their lived embodied spaces, places that are not restricted to physical boundedness. The current territorial construct protects physical space and in particular, the privacy of the home has "served as a sort of cultural shorthand for a broader privacy interest against exposure."[17] The home has been a presumptively private place originating in the common law of trespass in which "the house of everyone is to him as his castle and fortress, as well for his defence against injury and violence as for his repose."[18] The Supreme Court of Canada has repeatedly held that it can be presumed that Canadians legitimately expect what goes on in their homes to be private.[19] However, the jurisprudential focus on the sanctity of the traditionally defined physical home serves to diminish privacy protection by privileging the home and failing to take into account that the home does not just mean where we cook our meals and sleep at night. The privileging of the traditionally-defined home, and more specifically the inside of the home, undermines the spatial privacy interests we have in other physical contexts.

Although Canadian courts have found that a person has a reasonable expectation in locations other than in the home, including for example, in a hotel room,[20] inside a toilet stall in a public washroom,[21] as a tenant residing in an

---

17 Cohen, *supra* note 8 at 12.

18 *Semayne's Case*, 77 Eng. Rep. 194, at 195, 5 Co. Rep. 91a, at 91b (K.B. 1604).

19 See for example, *R v Patrick,* [2009] 1 SCR 579 at para 37 [*Patrick*]; *Tessling*, *supra* note 14 at para 41.

20 *Wong*, *supra* note 15; but note Justice Lamer's dissent that the hotel room ceased to be a private place when the defendant invited others into the room thus eliminating any reasonable expectation of privacy in that space.

21 *R v Flaherty* (1987), Nfld & PEIR 21 (Nfld. C.A.) [*Flaherty*]; *R v Silva* (1995), 26 OR (3d) 554 (Gen. Div.) [*Silva*]; but note *R v LeBeau* (1988), 25 OAC 1 (C.A.) [*Lebeau*] that there is no reasonable expectation of privacy outside the closed toilet cubicles of a public washroom.

apartment[22] and in a car if you are the owner,[23] these are still all places you can point to physical barriers sustaining its protection which reinforces the tangible boundary demarcating the inside-outside nature of the legal privacy protection. However, we engage in activities across a "plurality of realms",[24] increasingly so in a culture of ubiquitous and mobile computing. The lived spaces in which we expect to be free from observation and monitoring by police may be in a coffee shop, while engaged in a conversation on a train, while helping a neighbour in their front yard, when communicating with a colleague outside a university building or when interacting with someone using a device we carry in open view. Yet, the constitutional status of the physical home seems to be used as a fixed signpost to divert concern from these other spatial contexts and perhaps even justify finding a reduced expectation of privacy in contexts falling outside the home. Measuring privacy expectations by the inviolate home perpetuates a false dichotomy, in the emerging technological landscape, between the private and the public.[25]

The distinction between what is typically considered private and public is becoming practically less important and conceptually less useful.[26] Privacy, when using the peopled places construct, recognizes, in a way that the Supreme Court does not, that the private can happen in public. Peopled places supports dispensing with "rigid, formalistic borders between private and public spatial domains," instead attending to what constitutes a "reasonable expectation of privacy in a given context."[27] Moving the

---

22 *R v Pugliese* (1992), 52 OAC 280 [*Pugliese*], but not in common hallways of an apartment building, *R v Laurin* (1997), 98 OAC 50 [*Lauren*].

23 *R v Wise,* [1992] 1 S.C.R. 527 [*Wise*] but reasonable expectation is lower in a car than it is in the home.

24 Helen Nissenbaum, *Privacy in Context: Technology, Policy & the Integrity of Social Life* (Stanford, CA: Stanford Univ Press, 2010) 119.

25 The private and the public are not, sharply distinct categories, but instead, fluid, overlapping and contextual. See for example, Nissenbaum, *ibid*; Gary Marx, "An Ethics for the New Surveillance" (1998) 14:3 The Information Society 171; Gary Marx, "Murky Conceptual Waters: The Public and the Private" (2001) 3:3 Ethics and Information Technology 157; Elizabeth Paton-Simpson, "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places" (2000) 50 UTLJ 305.

26 For discussions on the history and nature of the public-private distinction, see Chapter Three, note 36.

27 Justice Gérard La Forest, "Opinion – Video Surveillance" (5 April 2002), online: Office of the Privacy Commissioner of Canada Archived News <https://www.priv.gc.ca/media/nr-c/opinion_020410_e.asp>. See also Nissenbaum, *supra* note 24, who questions the traditional public-private boundaries as an effective means to protect privacy.

discourse from simply determining whether it is a public or private place to the broader and lived spaces of everyday life provides a more nuanced contextual analysis to whether a privacy interest exists and whether it warrants legal protection.

Further, peopled places takes into account the changing nature of technology and the extent to which our conception of the home becomes much broader than traditionally conceived. The peopled places construct does not abandon spatial exclusion from the physical home, but instead builds on it by extending it to recognize, for example, that a "student's backpack is in effect a portable bedroom and study rolled into one."[28] And like a hotel room,[29] inside a public washroom toilet stall,[30] or in the sleeping area of a tractor-trailer,[31] the privacy interests arising in the ubicomp context share many of the same functions and attributes that are analogous to the privacy interests of the home. Our arrays of emerging technological devices are extensions of the home. In our mobile environment, these devices create new places of social intimacy. Permitting us to perform functions traditionally occurring only within the home, the reservoir of personal information created by these devices mirrors and captures our biographical core. Never leaving our sides and barely beyond our clutches, these devices are in many ways becoming the bedrooms of the ubicomp nation.[32] Ubiquitous technologies, either as devices we carry with us or as technologically embedded devices we interact with in our daily activities, create a context accommodated by peopled places.

In Rich Gold's analysis of ubicomp in 'This is Not a Pipe,'[33] he juxtaposes the painting of the pipe (as having the appearance of an ordinary pipe) with the ubicomp pipe, (which might be represented as a pipe but in fact incorporates a range of interactive functions that recontextualizes the pipe). Similarly, a smart phone, for

---

[28] *R* v *AM,* [2006] OJ No. 1663, Court of Appeal quoting CCLA submission, at para 50.

[29] *Wong*, *supra* note 15.

[30] *Flaherty*, *supra* note 21; *Silva*, *supra* note 21.

[31] *R v Nolet*, [2010] 1 SCR 851 (S.C.C.).

[32] Pierre Elliot Trudeau, former Canadian Minister of Justice, remark to newsmen, Ottawa, Canada, December 21, 1967 as reported in Geoffrey Stevens, "Bill Overhauls Criminal Code", *The Globe and Mail* (22 December 1967) 1.

[33] *Supra* note 2.

example, may look like only a telephone. However, because of its specific features and functionalities, and the uses by which people engage with it, the device is not only a cell phone, it also replicates functions traditionally associated with the home. For Gold, "[i]f Nineteenth-Century technology shredded the objective world into fine scraps, then ubiquitous computing can be thought of as the great integrator, collecting diverse pieces and behaviours and placing them back into single, if somewhat mongrelized boxes."[34]

The challenge, ultimately, is that a peopled places construct needs to be able to determine where one draws the peopled places line when an emerging surveillance technology cannot be assessed on the traditional inside-outside distinction. A useful starting point requires the addition of a second contextual dimension to the peopled places construct - the social context.

The Social Context

Placing privacy in the social context is not a new idea,[35] but in proposing the construct of peopled places for legal protection, the social context is approached from a different angle. First, in order to show the relevance of the social context for emerging ubiquitous computing and surveillance, this section begins by revisiting *Katz v United States*,[36] the American Fourth Amendment case upon which Canada's Section 8 privacy jurisprudence has been developed. The argument here is that *Katz* actually supports the peopled places construct, though this point has gone unnoticed through the obfuscation of the more famous "reasonable expectation of privacy" test. Second, after articulating the relevance of accounting for a shifting social context, reinforcing the

---

[34] *Ibid*.

[35] See for example, Nissenbaum, *supra* note 24; Steeves, *supra* note 16; Robert Post, "The Social Foundations of Privacy: Community and Self in the Common Law Tort" (1989) 77 Cal L Rev 957.

Note also that the social context is different from the phenomenological perspective. The focus of Phenomenology is on the experience of a sole person, whereas a sociological perspective focuses on the extent to which people are also created through social interaction. This dissertation takes the position that the experiential meaning of place is expanded by incorporating sociological insights.

[36] 389 US 347 (1967) [*Katz*].

importance of the peopled places construct is done by highlighting that the social context is at the heart of the interactive nature of emerging technologies.

In *Katz v United States*, acting on a suspicion that Charlie Katz was transmitting gambling information over the telephone to clients in other states, federal agents attached an eavesdropping device to the outside of a public telephone booth used by Katz. Based on recordings of his end of the conversations, Katz was convicted of illegal transmission of wagering information across state lines. On appeal, Katz challenged his conviction arguing the inadmissibility of the recorded evidence. The Court of Appeal, relying on *Olmstead v United States*,[37] rejected this argument noting the absence of a physical intrusion into the telephone booth itself. The United States Supreme Court ruled that Charlie Katz *was* entitled to Fourth Amendment protection for his conversations and that a physical intrusion into the area he occupied was unnecessary to bring the Fourth Amendment into play. Writing for the majority, Justice Stewart proclaimed the now famous words, "the Fourth Amendment protects people, not places."[38] This meant, he explained, that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection," but "what he seeks to preserve as private, even in areas accessible to the public, may be constitutionally protected."[39] For Justice Stewart, "[n]o less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[40] The implication is that we have privacy expectations in our lived spaces, including various social contexts outside the home, indeed even in "areas accessible to the public"—such as talking on the telephone in a public setting.

---

[37] 277 US 438 (1928); the 'trespass test' led the Court to conclude that wiretapping fell outside the ambit of the Fourth Amendment because it involved neither physical entry into the suspect's house nor an actual confiscation of the suspect's property.

[38] *Katz*, *supra* note 36 at 351.

[39] *Ibid.*

[40] *Ibid* at 352.

At issue in *Katz* was electronic monitoring of calls placed by a bookmaker from a telephone booth. Under the physicalist approach previously adopted in *Olmstead* – an analysis completely devoid of social context considerations – this clearly was neither a search nor a seizure. Nothing tangible was confiscated and there was no physical trespass. But the *Katz* court rejected this result as incompatible with "the vital role that the public telephone has come to play in private communication."[41] Recognizing the important social context of telephonic communications, the Court acknowledged that the nature of the "places" where we carry out our lives changes with the emergence of new technologies. The quintessential private place for communication had always been the home. However, as social practices began to shift with the proliferation of telephones, vital communications began to take place on wire-line telephones, including an expansive network of "public" telephone booths. Applying this contextual approach in modern times, the *Katz* decision (holding that there is a reasonable expectation of privacy in public telephone conversations) certainly paves the way for analogies to today's mobile telephones. Hence, technological changes widen the arena within which the presumption of a right to privacy ought to operate.[42]

Katz considered not just the question of whether electronic eavesdropping on telephone conversations is a search or seizure, and not just the question of whether a search or seizure requires a physical trespass, but also, implicitly, the broader question of the proper role of history in interpreting the Fourth Amendment. Justice Stewart's

---

41 *Ibid.*

42 The Supreme Court of Canada may be starting to recognize given its recent decision in *R* v *Telus Communciations Company*, 2013 SCC 16, [2013] SCJ No 16 (QL) [*Telus*]; In *Telus*, Owen Sound police obtained a general warrant under the relevant provisions of the *Criminal Code* requiring Telus to provide copies of any stored text messages sent or received by two Telus subscribers. Telus applied to quash the general warrant arguing that the daily acquisition of text messages from their computer database constitutes an interception of private communications and therefore, requires authorization under the *Criminal Code* wiretap authorization provisions. The Court found in favour of Telus, ruling that the general warrant was invalid since it purports to authorize the interception of private communications which requires judicial wiretap authorization. The interpretation of 'intercept a private communication' under the *Criminal Code*, should not, according to the Court, be dictated by the technology, but by the objective of protecting privacy interests in communication and should also be informed by the rights enshrined by section 8 of the *Charter*, which in turn must remain aligned with technological developments. Abella J. described text messaging as "in essence, an electronic conversation…the only practical difference between text messaging and traditional voice communications is the transmission process." (at para 5).Thus, going on to conclude that a text message is a private communication.

opinion for the Court in *Katz* was strikingly forward-looking, or at least present-looking as it reflected a change in the Court's entire approach to the Fourth Amendment, not just its thinking about what constitutes a search or seizure. It sought to modernize search and seizure law by moving away from its dependence on physical proprietary intrusion in order to recognize the realities of modern life; a shift from trespass to evolving notions of reasonable expectations of privacy. And perhaps the telephone booth itself is central to this shift.[43] In other words, it is the telephone *booth*, rather than simply the fact of the telephone *call*, that reveals a step toward recognizing the social context as a basis for protecting areas that go beyond property law. It is the telephone booth that brings the social function into practice. The physical embedding of telephone booths into streets, restaurants and buildings was evidence of the privacy expectations built into the social relationship of the call. For many years, the telephone booth was a lived space of incredible social experience. [44]

Telephone booth technologies developed in the *Katz* period required a series of expensive new innovations and infrastructures.[45] These were seen to be worthwhile because the embeddedness of phone booths in physical places enabled a new world of social activity, relations and norms to flow, almost magically, through the wires of telephones, creating intimate new places for social engagement that previously occurred only in the home. Today, with mobile and ubicomp technologies, these places are now embedded in the devices themselves. Consequently, social context also factors into peopled places to the extent in which it is embedded in the technology we are regularly coming to use in our everyday lives. Computing is, therefore, in some

---

[43] Katz, *supra* note 36 at 352; Although Justice Harlan's opinion is most well-known since he articulates the two-part reasonable expectation of privacy test, Justice Stewart's opinion describes the telephone booth in terms of the social world of activity, relations and norms, a web of meaning and exchange that goes on during calls placed from telephone booths.

[44] Tippi Hedren used one for protection in *The Birds*, film, directed by Alfred Hitchcock (Los Angeles, CA: Universal Pictures, 1963), see "Trapped in Phone Booth clip", online: movieclips.com <http://movieclips.com/Jtys-the-birds-movie-trapped-in-a-phone-booth/>; Maxwell Smart pushed a button in one to drop himself down to headquarters in *Get Smart*, television, NBC/CBS (1965-70), see "Get Smart title sequence", online: YouTube <http://www.youtube.com/watch?v=ElqZms_SUjg>; and Clark Kent had to hop into one to change his clothes in *Superman*, film, directed by Richard Donner (Burbank, CA: Warner Bros Entertainment Inc, 1978) ; college students competed in attempts to strain their capacity; as private enclosed havens, they were also used for doing business, homes and washrooms.

[45] Online Telephone History Museum: <http://thephonebooth.com/>.

respects, as much social as it is technical because the work that computation does and the uses to which we put it, are very much the sort of thing that social context helps us understand. Ubiquitous computing, in Weiser's vision, weaves itself into the fabric of everyday life. Part of the fabric of everyday life is the relationship between people, practices, society and the settings in which social activities take place.

The social context is reflected in the distinction between space and place and is, approximately, a distinction between the physical and the social.[46] Two settings with the same physical configurations may bring about quite different sorts of interactions due to the social meaning with which they are invested. For example, although a stage at an academic conference is physically configured in ways similar to a concert hall, it is generally not appropriate to get up and sing there. Similarly, classrooms and dining rooms can have similar arrangements, but we behave differently in them. Our behaviour in these environments is governed by social norms, not merely by physical constraints. So while 'space' refers to the physical organization of the setting, 'place' refers to the way that social understandings, or context, convey appropriate behaviour for that setting. It is why we hear the term 'out of place' rather than 'out of space.' This place-centric view turns the focus away from the structure of the space and towards the activities that take place there.

This view of the ways in which behaviour and activity depend on social context has been addressed by Erving Goffman, who drew attention to the ways in which people managed their conduct as a way of managing the impressions that others would form of them, and how, consequently, the ways in which they would conduct themselves will vary with the particular "audiences" for their conduct at any given time.[47] In this way, the public presentation of oneself involves restraint in the expression of emotions and attitudes, but sometimes we need to dispense with restraint and "be allowed to conduct ourselves in extremis."[48] If privacy "protects two

---

[46] Henri Lefebvre, *The Production of Space*, trans by Donald Nicholson-Smith (Oxford: Blackwell Publishing Ltd., 1991).

[47] Erving Goffman, *The Presentation of Self in Everyday Life* (Garden City, NY: Doubleday, 1959).

[48] Thomas Nagel, "Concealment and Exposure" (1998) 27 Philosophy & Public Affairs 3 at 19.

aspects of individuality: our ability to be distinct individuals and our ability to have an authentic inner life and intimate relationships,"[49] then privacy makes possible the construction of a public persona through which the individual can participate with those conventions that make social life possible. Moreover, the possibility of surveillance deprives the individual of control over how she presents herself to the rest of the world. Thus, privacy enables not only activities typically thought of as private, but also those typically thought of as public.[50]

What happens to social context and presentation of the self when interactive ubiquitous computing technology enters the picture? First, technology itself is part of the setting. Depending on the specific features of the technology and how they are used, they affect the conduct of our everyday action. For example, the ways in which electronic or digital communications have increased our connectedness to each other and access to information have changed our expectations about the availability of other people or information. Someone being 'out of touch' or 'offline' seems strange. Second, technology is increasingly the medium within which social activity takes place. We are used to the ways in which the physical world mediates our actions and forms a shared environment or when we are face-to-face, we understand how gestures and conduct appear. Computing technology as a medium for social conduct is inherently different because of its physically disconnected, representational nature. However, what this means is that the technology, rather than a physical space, is embedded with a set of social practices that give them meaning. It is a technologically-mediated social context, a lived space in which we attribute meaning.

2.3 Mobility and Peopled Places

Another feature of the peopled places construct is mobility in response to the shift in computing from sedentary to mobile access, connectivity and communication. The idea of a humanistic conception of place seems counter-intuitive to mobility.[51] In

---

[49] Lisa Austin, Privacy and the Question of Technology" (2003) 22 Law & Philosophy 119 at 147.

[50] Lisa Austin, "Privacy and Private Law: The Dilemma of Justification" (2010) 55 McGill LJ 165, 202-204.

[51] The *Oxford English Dictionary* defines mobility as "[a]bility to move or be moved; capacity of change of place; moveableness…also facility of movement." OED, 2nd ed, sub verbo "mobility".

other words, mobility unsettles that which is considered to be fundamental to conventional understandings of place; its very stability. If place is seen as a centre of meaning and field of care for people, as humanists assert, then mobility is the assumed threat to the rooted, moral, authentic existence of place.[52] Mobility, being on the move, suggests the absence of attachment and significance. Places marked by an abundance of mobility become 'placeless.'[53] For example, Edward Relph views modern tourism and superhighways as contributing to the destruction of place, and before highways, the railways contributed to destroying authentic senses of place.[54] He suggested that by "making possible the mass movement of people with all their fashions and habits" these spaces had led to the "spread of placelessness."[55] However, this dissertation, and in particular the building of peopled places, supports the position that mobility enhances rather than erodes a sense of place as lived meaningful experiences.[56] As we become more mobile and networked, place becomes less about the attachment and significance of the home, as traditionally defined, and more about how we form connections with the many sites in our lives. Mobile devices are connecting people in

---

[52] Andre Lemos, "Post-Mass Media Functions, Locative Media and Informational Territories: New Ways of Thinking About Territory, Place and Mobility in Contemporary Society" (2010) 13:4 Space and Culture 403-420; Edward Relph, *Place and Placelessness* (London: Pion, 1976).

[53] Relph, *ibid.*

[54] In a similar way, anthropologist Marc Augé has argued that the facts of postmodernity (he refers to supermodernity) point to the need for a radical re-thinking of the notion of place. For Augé, place has traditionally been thought of as a "fantasy of a society anchored since time immemorial in the permanence of intact soil" but such places are receding in importance and being replaced by 'non-places": *Non-Places: Introduction to an Anthropology of Supermodernity*, (London: Verso, 2008) 110. Non-places are sites marked by their transience and mobility, including freeways, airports, supermarkets- sites where particular histories and traditions are not, allegedly, relevant. In other words, unrooted places marked by mobility and travel. For example, Augé refuses to "dignify" certain locations such as the Los Angeles airport as a 'place' as such spaces permit individuals to have presence only by reason of passports, credit cards and airline tickets, undermining the human attachment to place. Joshua Meyrowitz similarly argues the decreasing importance of place and the corrosive effects on a sense of place because 'places' become less stable as more and more of personal experience and social relations become mediated by information and communication technologies and thus dis-embedded from their local context: *No Sense of Place: The Impact of Electronic Media on Social Behaviour* (New York: Oxford University Press, 1985) and "The Rise of Glocality" in Kristof Nyiri, ed, *A Sense of Place; The Global and the Local in Mobile Communication*, (Vienna: Passagen Verlag, 2005) 21; See also, James Kunstler argues that real interaction was being destroyed in the contemporary culture of media and transport: *The Geography of Nowhere* (New York: Touchstone, 1993).

[55] Relph, *supra* note 52 at 90.

[56] See for example, Doreen Massey, "A Global Sense of Place" in T Barnes & D Gregory, eds, *Reading Human Geography* (London: Arnold, 1997) 315-323; Noel Crabtree, "Place: Connections and Boundaries in an Independent World" in Nicholas Clifford et al, eds, *Key Concepts in Geography* (London: Sage Pblications, 2009) 153-171.

stronger and more personalized ways, not just socially, but also to place. If place is where we inscribe meaning then we are still in that place when we walk down the street interacting via a mobile device.

For Tim Cresswell, mobility without meaning is simply movement.[57] This is a particularly important point given the potential for surveillance of people's movements. Cresswell argues that mobility is movement imbued with meaning and the way movement gains meaning and significance occurs through what he calls the "production of mobilities."[58] Drawing on efforts to understand space in terms of its social and experiential dimensions, Cresswell aligns mobility as something akin to the idea of place; "[m]obility is the dynamic equivalent of place."[59] From this point of view, without meaning we are left with something rather superficial. We have simply movement. This is problematic because "movement is rarely just movement: it carries with it the burden of meaning."[60] Thus to ignore the way movement is entangled in all sorts of social significance is to simplify and strip out the complexity of reality as well as the importance of those meanings.

If mobility is simply viewed as movement from point A to point B, one way to visualize mobility is to see it as the action of simply getting from one place to another place. The line between point A and point B, the departure and arrival points, remains just that. But, as Cresswell puts it, "the bare fact of movement…is rarely just about getting from A to B."[61] What about the movement represented by the line that connects the two points together? Regardless of the line's supposed immateriality, it is "both meaningful and laden with power."[62] There is something in the space between the two points, something about the context of mobility that makes a vital difference. We can then visualize there is more than a line across a page from point A to point B, but

---

[57] Tim Cresswell, "The Production of Mobilities" 43 New Formations 11-25; and *On The Move: The Politics of Mobility in the Modern West* (London: Routledge, 2006).

[58] Cresswell, "The Production of Mobilities" *ibid*.

[59] Cresswell, *On the Move*, *supra* note 57 at 3.

[60] *Ibid* at 7.

[61] *Ibid* at 9.

[62] *Ibid.*

mobilities travelling over and through a complex terrain and topology of social spaces. And, following in the humanists' tradition, mobility then gains and is attributed meaning by those who interpret and make sense of it.

What this suggests is that location takes on more significance than just being a spot on the line between point A and point B. That line in between becomes important in light of the emergence of mobile location-aware technologies, which not only redefine people's connections to places, but also redefine the character of locations. Location acquires new meaning because it now becomes embedded with location-based information. In other words, locations are still defined by fixed geographical coordinates, but they now acquire dynamic meaning as a consequence of the constantly changing location-based information that is attached to them. Location is not inherently private information, but finding a location no longer means only finding its geographic coordinates, but also accessing an abundance of information that belongs to that location and is user-specific.

The web is all around us. We no longer 'enter' the web, but rather carry it with us. We access it via mobile, mapping and location-aware technologies. It is embedded in all sorts of sensors and networked devices. For example, mobile phones, GPS and RFID tags are location-aware technologies that mediate our interactions with networked spaces and the people in them. Our physical location determines the types of information we retrieve online and the people and things we find around us. Thus, we are more location-aware because we are connected in new ways through these technologies to the spaces and people around us. We can attach information to places, map our surroundings and connect to people around us. Being aware of location means being aware of all the information and people that exist in that location. And it means making different use of that location. The street is no longer limited to the perceptual horizon of the person walking down it. A network of information that is accessible through a mobile device augments it. Therefore, location-aware technology renders geography more fluid, but not irrelevant. Moreover, location information is not just longitude and latitude coordinates, but also encompasses who, what, when and where.

If mobility is not simply about getting from A to B, it should also be considered in terms of its fluidity. Like the fluid and permeable nature of the private-public divide, mobility in the peopled places construct is not dependent on fixed boundaries and fixed configurations among which we move. Rather, it encompasses flows and connectedness as opposed to nodes and separation. In this way, place is not defined only by Cartesian measures but also relationally, historically and meaningfully, in which people, along with their relationships and movements, determine the parameters of spatial lived experience. The values of mobility expressed in the vision of ubicomp go beyond a computational environment that one carries around as one moves about in the world. Peopled places takes in the kind of flexible reconfigurations and fluid accommodations that characterize the different experiences between people, technology and place.

In sum, ubiquitous computing will be everywhere. This is its essence, its explicit goal.[63] With it, privacy can no longer be understood as a local or domestic concept. My peopled places construct aims to help us recognize that privacy is no longer centralized but now distributed.[64] Rather than confining privacy to a territorial sphere or pigeonholing privacy interests into an artificial hierarchical classification scheme, the peopled places construct creates conceptual space for privacy to adapt to emerging social and technological places.[65]

2.4 Boundaries

Some sense of boundary is important in understanding peopled places because any notion of place that has no boundaries would empty the concept of its content. However, the current and enduring traditional private–public paradigm does not lend much needed theoretical or legal support in addressing the issues raised in this dissertation. Adhering to the traditional model that more sharply distinguishes between private space and public space is less and less useful to describe experiences

---

[63] See Chapter One, "What is Ubiquitous Computing" at p 27.

[64] This point is owed to Ian Kerr.

[65] See Chapter Three at p 121 discussing the hierarchical approach to classifying privacy interests as bodily, territorial and informational.

across the plurality of realms in our everyday lives. Yet as we move seamlessly between private and public domains, acknowledging the permeable nature of these concepts may be more productive than abandoning them altogether. Nothing is ever categorically private or categorically public, as those concepts are traditionally defined. And, as with all ideal-types, it is an analytical tool to facilitate thinking with and to help make sense of the world around us. Real world experiences, real world things, fall somewhere in between these two analytical endpoints. For example, consider a person engaged in a conversation with a neighbour in front of their houses. Something may be relatively more private or relatively more public, but it is never purely either. Privacy, when thought of as a condition of inaccessibility,[66] means that any point of the conceptual sliding scale has both a degree of privateness and a degree of publicness associated with it. This is why boundary management along with the private-public paradigm can work to support the construct of peopled places.

What then is boundary management and why is it embraced here and now? While traditional approaches have understood privacy as a state of withdrawal, at its core, a process of boundary management is based on Irwin Altman's model, which claims that managing privacy is about managing relationships between the self and others and between the self and space.[67] He refers to privacy as a "boundary regulatory

---

[66] See Chapter Three, Section 2.2 "Inaccessibility" at p 112.

[67] Irwin Altman, *The Environment and Social Behaviour: Privacy, Personal Space, Territory and Crowding* (Monterey, CA: Brooks/Cole, 1975). Similarly, for Alan Westin, privacy, when viewed in terms of the relation of the individual to social participation is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude of small-group intimacy or, when among larger groups, in a condition of anonymity or reserve. The individual's desire for privacy is never absolute, since participation in society is an equally powerful desire. Thus each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives: *Privacy and Freedom* (New York: Atheneum, 1970) 7. For discussions on Altman and Westin privacy theories, see for example, Stephen Margulis, "On the Status and Contribution of Westin's and Altman's Theories of Privacy" (2003) 59:2 Journal of Social Issues 411-429; and Valerie Steeves, "Reclaiming the Social Value of Privacy" *supra* note 16.

See also Sandra Petronio, *Boundaries of Privacy: Dialectics of Disclosure* (Albany, NY: State University of New York Press, 2002) who builds on Altman's model to develop a practical theory to explain the concealment and disclosure of information); Kirsty Hughes, "A Behavioural Understanding of Privacy and its Implications for Privacy Law" (2012) 75:5 Modern Law Review 806-836, who also draws on Altman's social interaction theory, as well as the 'inaccessibility' privacy theories to develop what she calls a "modified barrier theory" which is a right to respect physical, behavourial and normative barriers. Privacy

process by which a person (or group) makes himself more or less accessible and open to others."[68] When we regulate our accessibility to others, though, including the accessibility of information, objects, space and time, or anything else we deem private, we simultaneously regulate our relationships with them. Altman conceptualizes privacy then as the "selective control of access to the self."[69] Rather than static, Altman regards privacy as a dialectic and dynamic boundary regulation process where people optimize their accessibility along a spectrum of "openness" and "closedness" depending on context. Privacy becomes then "the negotiated line between the two."[70]

As a dialectic process, privacy regulation is conditioned by our own expectations and experiences and by those of others we interact with. As a dynamic process, privacy is understood to be under continuous negotiation and management, with the boundary that distinguishes privacy from publicity refined according to circumstance. This type of framework aligns with an experiential notion of place and resonates in the ubicomp context by virtue of its mobile and interactive nature. It also takes into account the problematic private-public paradigm inherent in the legal protection of privacy by moving away from characterizing the privacy interest as a fixed and enclosed space to one that is constantly negotiated within lived spaces. Kirsty Hughes' 'modied barrier' theory addresses the non-physical barrier breaches by advocating normative barriers where physical and behavioural barriers are inadequate.[71]

---

is experienced when barriers are respected and privacy invasions occur when a privacy barrier is breached; and Julie Cohen, *Configuring the Networked Self*, *supra* note 8, who relies on Altman's model to suggest boundary theory as a means of "re-imagining privacy." Technologists have adopted Altman's theory of interpersonal boundary negotiation process to address privacy concerns in the design of ubiquitous computing technologies: see for example, Leysia Palen & Paul Dourish, "Unpacking Privacy for a Networked World" in *Proceedings of the SIGCHI On Human Factors in Computing Systems* (New York: ACM Press, 2003) 129-136, who use Altman's model to define a technical framework.

68 Altman, *supra* note 67 at 10.

69 *Ibid* at 18.

70 Steeves, "Reclaiming the Social Value of Privacy," *supra* note 16 at 202. Conceptualizing privacy in this way not only promotes the development of intimate relationships, but also one's evolving sense of identity. If we effectively control the openness and closedness of self to others in response to our desire and the environment, we can, in Altman's view, function better in society than those who cannot. In order to regulate our privacy successfully, we need to use a variety of behavioural mechanisms, such as verbal cues, and environmental mechanisms of territoriality and personal space. (Altman, *ibid* at 77-79).

71 Hughes, *supra* note 67.

2.5 Summary

In summary, the construct of peopled places has been proposed as an alternative to the current territorial model, to better reflect the spatiality central to our experiences and expectations in everyday life. This construct seeks to provide a conceptual basis upon which more effective protection of the spatial privacy interests implicated by ubiquitous computing can be attained. Building on the idea of experiential place, this section has sought to articulate the essential characteristics of peopled places. Embodiment recognizes the body as a central reference point in our interactions with people, things and the environment. The physical and social contexts speak to how we live in the real, physical, structural world. At the same time, however, social context shapes the meanings and our interactions of both the physical and technologically-mediated environments. Mobility is a key feature of peopled places because, with increasing mobility, our movements and locations take on greater significance. This is particularly important when location-aware technologies facilitate tracking people's movements. And finally, to complete the conceptual model of peopled places, the symbolic stronghold of the traditional private-public distinction needs to make room for an interpersonal boundary regulation process.

Territorial privacy is informed by traditional definitions of space and place. Motivated by the limitations of this model for protecting privacy, this chapter is premised on a conception of 'place' as lived spaces, to better reflect the spatiality central to our lives. Part One provided the conceptual basis for a new privacy construct. Now that the conceptual construct of peopled places is formulated, what will it do for privacy law? Part Two of this chapter, beginning at Section 3 below, takes the peopled places construct and applies it in law to show how it can, and ought to, work to more adequately sustain core spatial privacy interests and the expectations that accompany them. Interests, as discussed and examined in earlier chapters, which are particularly vulnerable in the context of ubiquitous computing and surveillance. It concludes by suggesting how spatial privacy can work along-side, rather than be consumed by, informational privacy.

3. What 'Peopled Places' Does for Privacy Law

As a starting point, the construct of 'peopled places' seeks to enrich the protection of 'people' in the original articulation in *Katz* that privacy protects "people, not places." The concept of peopled places lends further substance to Justice Dickson's stated goal of section 8 privacy protection that the interests engaged by section 8 are not simply an extension of the concept of trespass, but rather are "grounded in an independent right of privacy held by all citizens."[72] As this section will show by way of examples, the peopled places construct furthers privacy protection by ensuring that any state interference with one's person, one's *lived* spaces or one's personal information respects her fundamental human dignity. Despite privacy's protean nature,[73] the peopled places construct would help ensure that privacy is understood as a fundamental component of personhood and integrally connected to self-fulfillment in a modern society, as vital to modern living as "oxygen is for combustion."[74] More importantly, peopled places offers a more concrete understanding of how privacy protection ought to be carried out in the ubicomp environment.

Although the Supreme Court of Canada has drawn explicit links between section 8 privacy and human dignity and personhood,[75] its continuing reliance on the three-zone taxonomy and physical intrusion under the territorial zone has, at best, emphasized people *in* places. What is important is not people *per se*, but people in particular places which fails to take into account 'people' as a meaningful category in its own right or the nature of social interactions. Moreover, a person-centered analysis has given way to an assessment of the nature and quality of information gathered.[76] Peopled places more clearly recognizes the underlying values privacy seeks to protect by creating a positive right rather than a negative right. In other words, peopled places in the constitutional context involves not simply a protection against invasion, but also

---

[72] *Hunter*, *supra* note 15 at 158.

[73] *Tessling*, *supra* note 14 at para 25.

[74] Charles Fried, "Privacy" (1967-8) 77 Yale LJ 475 at 478.

[75] See for example, *R* v *Plant,* [1993] 3 SCR 281 at 292 [*Plant*]; *R* v *Dyment,* [1988] 2 SCR 417 at 429 [*Dyment*].

[76] *Tessling*, *supra* note 14; *Gomboc*, *supra* note 14; *R v Nolan*, [1987] 1 SCR 1212 [*Nolan*].

protecting the capacity to do the things that makes one a person. Contrary to Margaret Radin's theory of property for personhood,[77] the physical home, for example, is not the only constituent of identity and self-development. Physical space is important only insofar as it secures the ability to expose or conceal different aspects of our self to others.[78] Thus, 'peopled places' is not grounded in the right of exclusionary control over a physical territory, but rather in the domain of spatiality, social interaction and boundary maintenance.

The remainder of this chapter provides legal examples that illustrate how the peopled places construct will better accommodate privacy interests in an environment of pervasive computing. By promulgating an approach that demands spaces to be understood not as empty vessels but as peopled places, it affirms the Supreme Court of Canada's long-standing intention to remedy the trespass theory of privacy by linking section 8 of the *Charter* to the protection of "people not places". The new approach of peopled places addresses the limitations of the current approaches as demonstrated in three significant ways. First, peopled places would protect people in their interpersonal relations regardless of location or proprietary ownership. Second, under the peopled places conception of spatial privacy, warrantless continuous vehicular surveillance without physical trespass would be considered an unreasonable search, and by extension, tracking people's movements through the use of ubiquitous computing technologies. And third, the current zonal classification scheme serves to marginalize spatial interests. Peopled places offer courts an apparatus to engage in a more effective analytical approach in the ubiquitous computing context where the traditional dichotomies for space, person and time are easily deconstructed.

3.1 Peopled Places and Interpersonal Relations

Embodied aspects of our lives can be inseparable from who we are and how we experience the world.[79] So when government surveillance seeks to control aspects of

---

[77] Magaret Jane Radin, "Property and Personhood" (1982) 34 Stanford Law Rev 957.

[78] Altman, *supra* note 67 at 103.

[79] Goffman, *supra* note 47.

our embodied lives, it may intrude into those aspects of our lives from which our experience of ourselves is inseparable. Similarly, personal relationships are inseparable from embodied relations with others. We share space with others, altering our behaviour by their mere presence, even in what is typically considered the most private conduct. How we act in the presence of others, what we reveal about ourselves to others, expose to others, establish boundaries between privacy and publicity.[80] Our embodied lives can be disrupted by government crossing the boundaries of our shared, yet private, lives.[81] This type of invasion is reflected in our technologically-embodied activities with others.

A generation of people today can and want to stay more closely connected with their close social network of friends. Utilizing her cell phone's GPS, Anne subscribes to the service that tracks her and her friends' whereabouts. With this service she can find her friends easily and they can find her. Friends do not have to wonder if she is currently at their favourite coffee shop. The phone will tell them. Neither Anne nor her friends intend to reveal to the entire world their whereabouts. Their phones help them keep track of their friends and family, their chosen close social networks. Through the same service, each of their phones will also inform the police of their location, should the police become interested. Police may effectively become part of Anne's social network, monitoring her movements just as if they were one of her friends. Moreover, when sitting in the coffee shop, Anne is located in a public space and police can conduct surveillance of her public movements.

These surveillance activities undermine the conditions of ordinary personal life shared in the company of others. Peopled places, unlike the current territorial model, captures a sphere of interpersonal relations that are constitutive of everyday life, a view of the world that recognizes the essential interconnectedness of people and the importance of intimacy in a variety of settings. Ordinary life involves sharing with other people in ways that are simultaneously private and public. A typical day for many

---

[80] Altman, *supra* note 67.

[81] Erving Goffman, "The Territories of the Self" in Relations in Public: Microstudies in the Public Order (New York:Basic Books, 1979) 23-32; Post, *supra* note 35 at 971.

will involve sharing thoughts, information, ideas, intimacies, conversations, company, friendships, places and public spaces. These activities are private to the extent that they may constitute a sphere of personal social relations. These activities are public insofar as they occur in public spaces such as offices, parks, restaurants, churches, streets and sidewalks. Thus, a single activity may entail both private and public aspects. A conversation with a friend on a park bench may be a private conversation insofar as it is not intended for public broadcast, but it is also public if a bystander happens to look or an eavesdropper happens to listen. Privacy and publicity do not define entirely separate spheres of life. Anne's participation in her cell phone social networking service illustrates the limited public, but still private, nature of ordinary life shared among friends. Her participation in the service reflects the value she places on staying connected with her close personal relations, but does not reflect a desire or expectation she has to make her movements known to the general public.

Fluid boundaries between what is private, though in the company of others, and what is genuinely public, even if unnoticed by others, shape how we live ordinary life. We define the boundaries of our relationships with others by both sharing with and withholding aspects of our lives. Undercutting the notion of privacy requires nondisclosure; the more we share, the more private and personal our relationships with others often become. By contrast, acts of exposure define our most public and impersonal relations with others. If public exposure forfeits privacy protection, then how section 8 privacy doctrine defines public exposure determines what aspects of ordinary life receive protection from government interference. What receives constitutional protection in turn shapes the boundaries of ordinary, everyday life.

The peopled places approach seeks to protect the interpersonal relationships constitutive of everyday life. Law enforcement, when engaging in surveillance activity anywhere, anytime, invades the wider private sphere of interpersonal relations by exploiting the vulnerability of our everyday lives. In other words, interpersonal relationships become sources of personal vulnerability. By gaining access to everything we share with others, whether it is information, conversations, networks, offices, coffee shops, homes or spaces, police are able to assume the position of the one with whom

we have exposed ourselves to. By assuming this position, police become present in the interpersonal relationships upon which people's privacy depends.

The conceptual complexity of privacy in relation to territoriality, rather than peopled places, lures us to think of privacy as applying to individuals in social isolation. Privacy, however, is also relational. It is, at least in part, experienced in relation to other persons through varying degrees of intimacy.[82] Intimacy requires sharing spaces, experiences, emotions, thoughts, information among other things with other people. This is, in essence, the lived spaces upon which the peopled places construct is built. Even if autonomy is a central feature of privacy, autonomous life is not life lived in isolation from others. When we engage in interpersonal relations, we leave what might be called isolated privacy to experience a form of privacy when with others, which occur everywhere. For example, protecting the homeowner, yet not the visitor to your home[83] reinforces proprietary ownership under the current model of territorial privacy. In *Edwards*, although the accused was a regular visitor to his girlfriend Evers' apartment and had his own key, he could not, according the Supreme Court, demonstrate an expectation of privacy sufficient to access the section 8 right to be free from unreasonable search or seizure. Although the existence of rights depended on the "totality of circumstances,"[84] greater weight was given to possessory interests, such as control of the property or place searched, ownership of the property or place and the ability to regulate access, including the right to admit or exclude others from the place.[85] This ignores the social realities of the context and the relationship of the parties. Similarly, in *R. v Belnavis*, the Supreme Court of Canada decided that as a passenger in the car, the accused had no reasonable expectation upon which to base a

---

[82] Charles Fried, "Privacy", *supra* note 74 at 485; James Rachels, "Why Privacy is Important" (1975) 4 Phil & Pub Aff 323, 329; Ruth Gavison, "Privacy and the Limits of Law" (1980) 89 Yale LJ 421, 450; Jeffrey Reiman, "Privacy, Intimacy and Personhood" (1976) 6 Phil & Pub Aff 26, 32; and Julie Inness, *Privacy, Intimacy and Isolation* (New York: Oxford University Press, 1992).

[83] *Edwards, supra* note 13 at 123.

[84] *Ibid* at 129.

[85] *Ibid*

section 8 claim because her connection to the car was extremely tenuous.[86] She did not own the car, have any control over the car and did not demonstrate any ability to regulate access to the car. This too ignores the reality of taking drives with a partner, child or friends, common and legitimate activities during which both drivers *and* passengers reasonably expect to be free from unwarranted police intrusion.

These cases undermine the fact that section 8 of the *Charter* applies to everyone. Treating privacy as one-dimensional, and the home or car owner's interest in the privacy of her home or car as paradigmatic, effectively denies to all of us protection for a different dimension of privacy that is just as important for the conduct of our lives. Further, these cases disavow the spirit of *Hunter* — intended to protect people — and are contrary to its claim that section 8 is to be read purposively and given a large and liberal interpretation.[87] Intimate relationships and other social interactions necessarily require some degree of reduction in the expectation of privacy among individual members of the relationship or interaction, but they should have no less right to be free from warrantless searches. Peopled places does not depend solely on proprietary ownership, but rather, would protect the reasonable expectation of privacy people have when engaged in their interpersonal relationships regardless of *whose* property is searched. For example, under the peopled places approach, a guest in a home, or a passenger in a car could assert a reasonable expectation of privacy that is not dependent on the ability to establish a possessory right. Police could not enter your home, for example, without a warrant on the basis that the guest has no reasonable expectation of privacy nor gather evidence admissible against the guest as long as they did not charge the home-owner.

Moreover, the consequences of public visibility can be avoided only by hiding from view, ourselves, our interactions with others and those items of information one wishes to keep private. This means our privacy expectations are interpreted as

---

[86] *Belnavis*, *supra* note 14; see also, for example, *R* v *Harrison,* [2009] 2 SCR 494, a case involving the accused and his friend who were driving a rental SUV from Vancouver to Ontario and were stopped by police for an incorrect license plate violation, the court finding that the passenger had no reasonable expectation of privacy in the vehicle rented in his friend's name.

[87] *Hunter*, *supra* note 15 at 106.

reasonable only when connected to particular places in which it is possible to physically, and literally, barricade ourselves from exposure. This view ignores that we often have expectations of privacy that we share with others when we are in each others' presence, without hiding from view, but nevertheless do not expect to be performing for all the world, and certainly not for law enforcement. Using peopled places moves the section 8 jurisprudence from a static view to a more nuanced view of privacy by drawing the line not only at the threshold of the home, but also around people's interpersonal relations.

If section 8 remains static, privacy is rendered consistently vulnerable to technological changes. For example, social networking technologies and practices produce new opportunities for government surveillance and intrusion. In the case of a large social network of 'friends' and relatively impersonal interactions between them, perhaps there is less reason for concern. Consider actions taken in a public park with a group of friends. A person could not expect the police to shield their eyes from readily observable public conduct. However, not all social networking is impersonal, and not all networking is like actions in the park. Recalling the scenario where Anne signs up for a social networking service allowing her to locate all of her friends,[88] Anne's activity is not easily analogized to actions in the park, and her expectations are not that she has revealed her location to the world. Rather, her choice of privacy settings on her social network may well have been set up to intermediate a relatively closed network of friends who mutually agree to reveal their whereabouts to each other, but not to the world at large. The new approach to spatial privacy would give courts the ability to draw distinctions among different forms of interactions, treating the interpersonal differently than the impersonal.

For example, informal rules of looking seem to make this point. Briefly looking at someone else permits the initial gathering of visual information without either party committing to further interaction. Two parties who recognize one another or want to invite more intimate contact may mutually consent to longer and more frequent

[88] See original scenario above, "Peopled Places and Interpersonal Relations" at p 195.

looking. But looking too long, too intently or too often becomes staring. Staring violates what Erving Goffman called the rules of "civil inattention," those "things that, though perceived, are not deemed to have been seen or heard."[89] Similarly, the forced close quarters of a crowded elevator make more than the briefest of glances invasive.[90] Who looks at us, how they do so, for how long, and for what purposes, matters. When technology enables the government to stare with an ever-vigilant eye, seeing is transformed into observing, elevating the potential privacy harms as the boundaries of the self dissolve, and by extension, the privacy of interpersonal relations is compromised.[91]

3.2 Peopled Places and Continuous Surveillance

One of the most pressing issues with respect to constitutional privacy protection is the extent to which law enforcement surveillance activity is enhanced by ubiquitous computing technologies. This is significant because ubicomp facilitates tracking our movements in public, not just watching us at a given location. Even current electronic tracking devices, such as GPS, potentially improve human perceptual abilities and enable the government to hear, see and otherwise learn more about people that was previously inaccessible. There is nothing necessarily sinister or inherently objectionable about government taking advantage of technological progress. Indeed, there are compelling and legitimate reasons to support uses that promote greater safety and security by making law enforcement more efficient.[92] However, emerging technologies overcome many of the limitations inherent in the passive mainstream technologies by tracking people automatically, remotely,

---

89 Erving Goffman, *Behaviour in Public Places* (NY: Free Press, 1963) 85.

90 *Ibid* at 137-138.

91 In the online context, Monu Bedi argues that the concept of interpersonal privacy should apply to social networking relationships because they are just as 'real' as their face-to-face counterparts: "Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply" (2013) 54:1 BCL Rev 1.

92 Steven Penny, "Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach" (2007) 97 J Crim L & Criminology 477; see also Queens University Surveillance Project, "Location Technologies, Mobility, Surveillance & Privacy" (March 2005) Report to the Office of the Privacy Commissioner of Canada (describing the public interests surveillance serves); and Jennifer Chandler, "Privacy Versus National Security: Clarifying the Trade-Off" in Kerr, Steeves & Lucock, *supra* note 16 at 121.

accurately, continuously in real time and in the real physical world, thus enhancing the ability to conduct surveillance without physical intrusion. This applies not only to remote tracking enabled by built-in vehicular GPS, but potentially to all our movements, inside or outside a car, as a result of embedded computing in the devices we carry with us combined with RFID, sensor and wi-fi technologies. Similarly, the use of drones provides yet another layer of surveillance along with thermal imaging of the home, GPS vehicular tracking, and location-aware cell phones, none of which require physical intrusions to conduct surveillance. The question then is whether the use of enhanced tracking capabilities circumvents the protection of privacy safeguarded by section 8 against unreasonable searches. In other words, does technology-enhanced surveillance change the nature of what constitutes a search for the purposes of section 8 of the *Charter*?

In Chapter Three it was suggested that technology can change the nature of what constitutes a search because more of our lives are potentially caught within a web of constant accessibility rendering irrelevant protections afforded by the traditional analysis. Legal approaches, largely relying on a territorial model, do not get at the core of what is ultimately objectionable; our desire, and expectation, to limit intrusions into peopled places without the threat of being watched and exposed. The Supreme Court of Canada's decision in *R v Wise* [93] and more recently, *United States* v. *Jones*,[94] both cases involving vehicular surveillance by police, illustrate the current deficiencies in law to adequately address the complex relationship between technology, searches and spatial privacy interests.

In *Wise*, the Crown sought to introduce evidence of the accused's whereabouts obtained through the use of a tracking beeper installed in his car.[95] The accused had

---

[93] *Wise*, *supra* note 23.

[94] 132 S. Ct. (2012) [*Jones*].

[95] A beeper is a small telecommunications device, basically a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver. By using a receiving device to monitor signals from a beeper, police can determine the beeper's general direction relative to the receiver's location. Beeper-assisted surveillance, therefore, requires police follow the targeted vehicle. Mark Monmonier, *Spying With Maps*: *Surveillance Technologies and the Future of Privacy* (Chicago, Ill: University of Chicago Press, 2002); JK Peterson, *Understanding Surveillance Technologies: Spy Devices, Privacy, History and Applications* (Boca Raton, FLA: Taylor & Francis, 2007). Beeper technology and GPS

been under surveillance for some time since police suspected him of involvement in a recent murder believed to be linked to a series of similar killings. They had obtained a warrant to search his home and vehicle, but had found nothing to link him to any of the homicides. The police towed the car to the police station to carry out the search. While it was there, but after the warrant had expired, they installed the beeper. The Supreme Court of Canada found the warrantless installation of the beeper constituted an unreasonable search thus violating section 8 of the *Charter*. However, despite the *Charter* violation, the evidence gathered as a result of the beeper was admissible because the search was minimally intrusive and therefore would not bring the administration of justice into disrepute.[96] Driving is a highly regulated activity for which, according to Justice Cory, "a reasonable level of surveillance of each and every motor vehicle is readily accepted, indeed demanded, by society."[97] Justice Cory concluded that a reduced privacy interest in cars on public roads combined with the use of an unsophisticated device was only minimally intrusive. The reasoning underlying *Wise* is if one can be seen by driving on public roads, it is implicitly acceptable to monitor that person and beeper technology simply augments physical visual surveillance that is otherwise permissible without legal authorization.[98]

In *Jones*, the United States Supreme Court held that the installation of a GPS device to monitor movements for 28 days constituted a violation of the Fourth Amendment's prohibition against unreasonable searches. The *Jones* majority, led by Justice Scalia, decided the issue on the technical narrow grounds of trespass finding police physically invaded the defendant's property by attaching the GPS device to his car without a warrant.[99] Justice Alito, concurring, argued that the long-term monitoring

---

devices serve essentially the same purpose: determining location. However, GPS tracking does not require any visual surveillance by police after the receiver has been installed. GPS technology is more sophisticated in that it is capable of remote, real time target tracking continuously for prolonged periods of time.

96 *Charter*, s 24(2).

97 *Wise*, *supra* note 23 at para 6.

98 This is, effectively, the public exposure doctrine: there is no privacy interest in what we voluntarily expose or disclose in public. *Tessling*, *supra* note 14 at para 39 (no reasonable expectation of privacy in the information because the heat loss released "off-the-wall" from the home was a "voluntary exposure of information.").

99 *Ibid* at 952-953.

was a violation of the defendant's reasonable expectation of privacy.[100] In other words, Alito J. would apply the *Katz* privacy-based approach rather than the property-based approach to resolve the case, asking whether the use of GPS tracking involved an intrusion a reasonable person would not have expected. Under his approach, "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable."[101] However, the use of "longer-term" GPS monitoring will more likely violate the Fourth Amendment.[102] Justice Alito declined to create a rule for determining at what point police tracking crosses this constitutional line, but concluded that four weeks was a search.[103] The split reasoning reveals on-going uncertainty, as in *Wise*, about the broader questions; in particular, how to constrain police and government discretion to conduct continuous surveillance that ensures the protection of people against unreasonable searches.

While we may expect a reasonable level of surveillance[104] on public roads to ensure compliance with the regulatory scheme, there is a quantitative and qualitative difference between the risk that your vehicle will be observed, even watched, by police for the purpose of road infractions and the risk that a device will track the vehicle and hence, the movements of people as they carry out their everyday lives.[105] Moreover, current approaches suggest that as a search moves away from a person's home, it becomes more likely that the person has voluntarily consented to have their

---

100 *Ibid* at 958.

101 *Ibid* at 964.

102 *Ibid*.

103 *Ibid*.

104 It is not made clear in *Wise* what the scope of a "reasonable level of surveillance" is. If it is meant to refer to police watching the roads generally for the purpose of determining vehicular and drive compliance or following a driver for a short period of time with the intention of stopping that vehicle, then it more likely falls within our expectations while travelling on the public roads. However, on Justice Cory's reasoning, it could potentially encompass police deciding to engage in longer more focused vehicular surveillance. Subject to exigent circumstances, this type and degree of surveillance reaches beyond what we would normally expect while travelling in our car.

105 It is useful to recall that the purpose of section 8 is to prevent unjustified searches. The *Charter* was "intended to constrain governmental action inconsistent with those *Charter* rights and freedoms; it is not in itself an authorization of state power." *Hunter*, *supra* note 15 at 156. Thus, police conduct that extends beyond monitoring the roads in the course of regulating or observing what goes on there, without a valid warrant, runs contrary to the purpose of section 8.

movements being watched. When people travel on streets or highways, whether in a car, on a bus, in a taxi or on foot, they do voluntarily subject their movements and behaviours to observation. However, systematic surveillance is inconsistent with our lived experiences because individuals routinely carve out peopled places in public spaces in which, and during which, we expect to be free from on-going observation by law enforcement. As Daniel Solove points out, "[a]ccording to the prevailing view of the law, if you're in public, you're exposing what you're doing to others, and it can't be private."[106] This prospect of constant potential for exposure has led Solove to critique the 'no privacy in public' rule as a "binary understanding of privacy" that is both antiquated and inadequate.[107]

There is, as well, a distinction between knowingly exposing oneself to casual public view, and surveillance that is not contained by space or time. Comprehensive monitoring and surveillance of our movements reveals patterns, associations and activities that would not be apparent to casual observation.[108] Surreptitious monitoring of people's movements in a systematic and detailed manner raises new concerns with respect to informational privacy, but this kind of intensive surveillance also destabilizes personal spheres and the privacy expectations that go with them by compromising peopled places; lived spaces people experience when they leave their homes. Ultimately, when law enforcement can take control over information about us anywhere, anytime, they take away control over our spatial privacy.

Although Justice Alito's opinion in *Jones* recognizes the risk GPS poses to this loss of control over privacy, the distinction he draws between short-term and long-term surveillance defines when a search occurs in public space. It is questionable what length of time could be fixed for the purposes of making a section 8 determination, but

---

106 Solove, *Understanding Privacy* (Cambridge, MA: Harvard University Press, 2008) 110.

107 Solove, *The Future of Reputation: Gossip, Rumour and Privacy on the Internet* (New Haven, Connecticut: Yale University Press, 2007) 7.

108 See for example, Nissenbaum, *supra* note 24; Reiman, *supra* note 99; Teresa Scassa, "Information Privacy in Public Space" (2010) 7:2 CJLT 193; Elizabeth Paton-Simpson "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Spaces" (2000) 50:3 University of Toronto Law Journal 305; Gary Marx, "What's New About New Surveillance: Classifying for Change and Continuity" (2002) 1:1 Surveillance & Society 9.

even if it could be done practically and legally, the duration should not matter. Whether the length of the surveillance is short-term or long-term, continuous and constant tracking enables police to track people everywhere they go. While vehicular tracking would primarily occur in public view, embedded GPS in cell phones, for example, would mean that police could track people as they move to and from, in and out, of areas such as the home. Moreover, although prolonged surveillance captures a totality of behaviour and activities potentially revealing a more comprehensive picture of the person being tracked, a single journey can likewise reveal intimate details of a person's life. People's public movements typically reveal only mundane information about them, but this is not always true. Where we go are not necessarily just locations, or points on a grid. For example, many people would not want it known that they had visited a psychiatric institution, needle exchanges or a religious gathering. Obtaining this kind of information invades a reasonable expectation of privacy because it relates to a "biographical core of personal information" revealing "intimate details" of "lifestyle or private decisions."[109] GPS or other tracking technologies potentially reveal a great deal about non-criminal activity. This is true whether the surveillance is long-term or short-term.

And finally, grounding the determination of whether police conduct constitutes an unreasonable search in trespass theory has already been identified and discussed in Chapter Three, and section 3.2 of this chapter, as inadequate for the protection of privacy interests. Relying on a proprietary basis also points to the larger issue courts face, and which was not addressed in either *Wise* or *Jones*; how to protect privacy where there is no physical intrusion. Formulating an effective test in response is problematic because, in part, current privacy jurisprudence derives from the claim that when a technological device capable of augmenting human perceptual capacities is used to perceive no more than what could have been perceived lawfully by means of unaided human senses, it does not jeopardize section 8 privacy interests.

---

[109] *Plant, supra* note 75 at para 20; *Tessling*, *supra* note 14 at para 25.

By adopting a peopled places approach, courts would not necessarily differentiate between searches using technology and searches with the naked eye. Once one understands that places are peopled, it is easier to understand why a police officer who continuously watches an individual walking down the street to see what transpires may be conducting a search whether with unaided vision, binoculars, closed-circuit television or a drone. This approach avoids the problem of making assessments of the method used, as for example, whether the technology is in common use,[110] enhances the normal capacity of the police,[111] or whether and to what extent a physical intrusion is involved.

In sum, both *Wise* and *Jones* acknowledge that continuous surveillance without legal authorization may constitute an unreasonable search, but they also reflect the extent to which courts struggle with this issue, falling back on a territorial model grounded in proprietary interests and in traditional notions of physical space to assess intrusive practices by police. This type of analytical framework leads to an absolutist approach to the effect that there can be no privacy in public. Peopled places offer a conceptual basis upon which spatial privacy interests can be taken into account when assessing whether police surveillance activity is a search. Unlike a territorial construct, peopled places gives effect to privacy being interpreted more broadly to encompass

---

[110] *Tessling*, *supra* note 14 at para 10; in *United States v Kyllo*, 533 US 27 (2001) at 34, the United States Supreme Court used similar language: "not in general public use." The 'common use or general public use' caveat raises another issue. For example, Assuming RFID technology becomes ubiquitous, and that many RFIDs will remain activated, our ability to use this advancing technology will reduce our expectations of privacy. It will enable increasing, systematic and covert localization of individuals on a much wider scale. This substantially impacts people's traditional reasonable expectations of privacy in movement; they may have been visible at a certain time at a certain place, but much less traceable for a longer period of time. The overall result is that more of our lives, in more places, are exposed. The reasonableness of our privacy expectations in movement is diminished the more localization becomes a common side-effect of technology. It is not difficult to reduce reasonable privacy expectations by first eliminating the privacy, then the expectation of that privacy and, last, the reasonableness of our expectation of privacy. If society has no subjective expectation of privacy, because in fact, it has no privacy, then any claim to privacy would be objectively unreasonable to society as a whole. The eroding effect of technology on privacy is a slow, hardly perceptible process. There is no precise stage at which one can point to the use of technology as unreasonably tilting the balance of privacy. However, because of the fluid and flexible nature of privacy, society has been and will continue gradually to adapt to new technologies and to the privacy expectations that go with them.

[111] *Tessling*, *ibid* at para 39 – 41; see also Justice Abella's Ontario Court of Appeal decision in *R v Tessling* [2003] OJ No. 186 (QL), 171 CCC (3d) 361, 63 O.R. (3d) 1 (C.A.) (finds that police use of FLIR technology constitutes a search of the home because it was used to gather information about inside the home that would not otherwise be available by the naked eye).

lived spaces. Through its application, courts would be able to recognize a reasonable expectation not to be subject to continuous and targeted surveillance without legal authorization, regardless of location, duration or technique used.

3.3 Peopled Places & Zonal Classification of Privacy Interests

Chapter Three canvassed the three categories of privacy interests employed by the Supreme Court of Canada that may be implicated by a police search: personal,[112] territorial[113] and informational.[114] These zones, or dimensions, are meant to go some way towards accounting for and describing the underlying interests that privacy, as formulated under section 8 of the *Charter*, purports to protect. While initially appealing as a conceptual device, this hierarchical classification system is less effective in the ubiquitous computing context because, as discussed in Chapter Three, the use of enhanced surveillance technologies by law enforcement increasingly blur the lines among these privacy zones. Where the privacy interests implicated by police surveillance do overlap, the outcome may be dictated by the analytical approach of the court, not an insignificant, since how the privacy interest is classified will potentially lead to a very different result. This has serious implications for an already shrinking

---

[112] This category protects "[p]rotects bodily integrity, and in particular the right not to have our bodies touched or explored to disclose objects or matters we wish to conceal." *Tessling*, *ibid*, at para 21.

[113] The original notion of territorial privacy protected the home (''the house of everyone is to him as his castle and fortress'' *Semayne*, *supra* note 18, an interest that has consistently been upheld, at least in theory. See for example, ''[t]here is no place on earth where persons can have a greater expectation of privacy than within their 'dwelling-house.''' *Tessling*, *ibid* at para 22.

[114] This category is "predicated on the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain…as he sees fit." *Tessling*, *ibid* at para 23.

In *Plant*, *supra* note 75 at para 20, Sopinka, J. delineates the scope of the informational privacy interest as "protecting a "biographical core of personal information" including "information which tends to reveal intimate details of the lifestyle and personal choices of the individual." In *Tessling*, Binnie J. concludes that "[e]xternal patterns of heat distribution on the external surfaces of a house is not information" in which there is a reasonable expectation of privacy…" (at para 63) because, in part, "the information gathered by FLIR technology was, on its own, 'meaningless.' (at para 58); and in *Gomboc*, Deschamps J. applies the 'biographical core' premise of *Plant* and *Tessling* minimizing the significance of electrical consumption gathered by the Digital Recording Ammeter (DRA) determining the disclosure "has no greater impact than the unprotected electricity records in *Plant* or the heat emanations in *Tessling* (at para. 35). The dissenting opinion in *Gomboc* rejected the application of *Plant*, as DRA predictions "do have the potential to reveal 'private or biographical information" (at para 128) going to conclude that residential electricity consumption is not meaningless or mundane information (at para 133).

zone of territorial privacy.[115] Building on similar reductionist arguments,[116] it is further argued that by adopting an analytical approach reduced to just information, it marginalizes the spatial dimension of privacy and further, risks spatial privacy interests being collapsed into the informational paradigm. For example, *Tessling*, *Gomboc* and *Patrick* all engaged privacy interests involving the home, but were decided on the basis that the interests implicated were essentially informational.[117] In other words, there was no actual search of the home itself diminishing the importance of the territorial privacy interest.

The Supreme Court of Canada has consistently recognized a heightened expectation of privacy in the home.[118] In recognizing this heightened expectation of privacy in the home, the law has used "the notion of place as an analytical tool to evaluate the reasonableness of a person's expectation of privacy."[119] However, the conception of place the court has employed in making this evaluation is fundamentally concerned with expectations people have in traditional bounded geographical places and direct visual observation from the outside. In other words, unless police trespass, they cannot see what is going on in the home. Where there is no physical intrusion courts have been unable to find an alternative basis upon which to sustain the heightened expectation of privacy in the home. Instead, courts have shifted the focus of its analysis from an expectation of privacy in the place searched to expectations about the accessibility of information about activities occurring in that place. This shift has

---

115 *Tessling*, *ibid*; *Gomboc ibid*; *Patrick*, *supra* note 19.

116 On information reductionism, see Jena McGill and Ian Kerr, "Reduced to Absurdity: Reasonable Expectations of Privacy and the Need for Digital Enlightenment" in Jacques Bus et al, eds, *Digital Enlightenment Yearbook 2012* (Amsterdam: IOS Press, 2012) 199; Jane Bailey, "Across the Rubicon and into the Apennines: Privacy and Common Law Police Powers after *A.M.*and *Kang-Brown*" (2009) 55 Crim LQ 239 and "Framed by Section 8: Constitutional Protection of Privacy in Canada" (2008) 50:3 CJCCJ 279; Ian Kerr & Jena McGill, "Emanations, Snoop Dogs and Reasonable Expectations of Privacy" (2007) 52:3 Crim LQ 392; Teresa Scassa, "Information Privacy in Public Space" *supra* note 128 at 193; and on social context reductionism, see Valerie Steeves, "If the Supreme Court Were on Facebook: Evaluating the Reasonable Expectation of Privacy Test from a Social Perspective" (2008) 50:3 CJCCJ 331.

117 *Tessling*, *supra* note 14 (no reasonable expectation in heat emanating from the home); *Patrick*, *supra* note 19 (no reasonable expectation of privacy in garage at property line); *Gomboc*, *supra* note 14 (no reasonable expectation in residential electrical use).

118 *R v Evans*, [1996] 1 SCR 8; *R v Silveira*, [1995] 2 SCR 297; *R v Feeney* [1997] 2 SCR 13 and in *Tessling*, *ibid*; *Patrick*, *ibid*; and *Gomboc*, *ibid* the court acknowledged a territorial privacy interest involving the home.

119 *Tessling*, *supra* note 14 at para 22.

meant that police can fly over your home using FILR technology to measure a home's heat consumption, go through garbage taken from inside the home property line and use a Digital Recording Ammeter to determine patterns of domestic electricity consumption, all without a valid warrant. The immediate effects are to undermine the ability to protect any interests in controlling information relating to the home. The longer-term implications to further erosion of the spatial dimension of privacy are more unsettling as the home becomes increasingly 'smart.'[120]

In its adaptation to home use, surveillance technology retains many of the traits that characterize similar tools used in the public sphere. Yet, because monitoring systems or embedded household objects are voluntarily installed by residents of the home, it becomes "both a manifestation and an agent of meaning that is formed by its users and by its locale."[121] Similarly, personal and home robots facilitate direct surveillance and access to the home and information, yet the harms are more complex to assess when considered social robots.[122] In these circumstances, under the current approach in law to adopt an informational analysis to assess the reasonableness of a search, since there is no physical trespass by police, the privacy interest we have when a device is physically inside the home to observe people and things is not protected. Indeed, these are devices located *inside* the home, albeit voluntarily, and not just devices on the outside capable of peering into the home. This leaves the informational privacy interest to be evaluated which, given the court's increasingly narrow interpretation of information, effectively strips people of any privacy protection.[123]

---

[120] Recall the Smart Home, see Chapter Two at p 84, and Ambient Intelligence, see Chapter One at p 60. Most current surveillance systems for home use have been developed and marketed as a more effective means for protecting family and property, as for example, networked home security systems and on-site health monitoring services, but in-home everyday devices, embedded with computing technology, from consumer products to household appliances will also take on surveillance capabilities, as for example the smart refrigerator broadcasting its contents via networked connections.

[121] Adam Swift, "Locating 'Agency' Within Ubiquitous Computing Systems" (2007) 8 Int. Rev. of Info. Ethics 36 at 38; see also Adam Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing* (Berkeley, CA: New Riders, 2006) 148-150.

[122] M. Ryan Calo, "Robots and Privacy" in Patrick Lin et al, eds, *Robot Ethics: The Ethical & Social Implications of Robotics* (Cambridge, MA: MIT Press, 2012) Chapter 12, 187; Ian Kerr, "Bots, Babes and the Californication of Commerce" (2004) 1 Ottawa Law and Technology Journal 285-325.

[123] The scope of the informational privacy interest, in particular the biographical core construct has become too malleable: Bailey, *supra* note 135; McGill & Kerr, *supra* note 135; See also, Tim Quigley, *Procedure in*

Reconceptualizing territorial privacy as peopled places contributes to a more effective framework for classifying privacy interests. For example, the home context illustrates this point; as surveillance technologies are brought into the home, they destabilize the notion of home as a lived space by situating it in a network of visibility. The device is a proxy for human, or police, presence. Seen from practically anywhere through wireless connectivity and accessible at any time, the home becomes segmented into observable and monitored spaces in which people are captured as digitized images. Surveillance facilitates the reading of sites, and people, as data – making it easier for courts to characterize the privacy interest as informational. Peopled places provide a richer context to more adequately assess privacy interests involving the home rather than reducing people and their information to bits and bytes of heat, electricity or trash. In other words, it recognizes the distinct spatial experience that is the home.[124] As peopled places, to be seen entails a loss of privacy, both in terms of the ability to determine when, how and to what extent information about you is disclosed,[125] or "…the condition in which others are deprived of access to you."[126] Such a loss of privacy threatens the sense of control one may have over information, as well

---

Canadian Criminal Law, 2nd ed (Carswell: Toronto, 2005), "[u]fortunately, whether a biographical core of information deserves privacy protection has sometimes served as a mask for extending police powers" (at p. 8); William MacKinnon, "Tessling, Brown and A.M.: Towards a Principled Approach in Section 8" (2007) 45 Alta L Rev 79 who advocates a return to a principled approach to test privacy claims against technologically enabled intrusions as articulated by LaForest J. in *Wong supra* note 20; and Don Stuart, *Charter Justice in Canadian Criminal Law*, 5th ed (Carswell: Toronto, 2010) at 271 who suggests, in response to *Tessling*, the question should be "whether occupants of houses have a reasonable expectation of privacy from police inspection from aircraft using technology devices, however crude." This would reframe the question then to whether residents of a home have an expectation that their activities will not be observed and scrutinized by police using a surveillance technology without physical intrusion without a warrant. This way the home can still be examined but legal authorization would be determined based on balancing the interests between government's interest in criminal investigation and the residents' privacy interests. This would better address "the aggregation of information in an era when advancing technology will mean a greater threat to personal privacy." (MacKinnon, at 80).

[124] Drawing on parallels that set it akin to the body itself, phenomenological approaches, as discussed in Chapter Four, point to the home's capacity to offer a site for where one can, first and foremost, be one's self: Gaston Bachelard, *The Poetics of Space: The Classic Look at How We Experience Intimate Places*, translated by Maria Jolas (New York: Orion Press, 1964); Maurice Merleau-Ponty, *The Phenomenology of Perception*, translated by Colin Smith (New York: Routledge Press, 1958).

[125] Westin, *supra* note 68.

[126] Jeffrey Reiman, "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future" in Beate Rossler, ed, *Privacies: Philosophical Evaluations* (Palo Alto, CA: Stanford University Press, 2004) 194, 197.

as over access to the person.[127] Therefore, peopled places create the condition for spatial privacy to consider the privacy interest we have in not being exposed by visual and informational surveillance.

And finally, adherence to the current zonal classification makes it virtually impossible to recognize any spatial privacy interests in public. The peopled places approach provides a way to move beyond the tightly confined classifications in order to better reflect the plurality of realms we live and where surveillance now operates. Its central dimension is not the ability of people to share intimate information, but rather simply, to carry on their everyday lives. What makes searches intrusive is not merely the fact that intimate details of a person's life may be brought into public view, though it is very often a concern. Rather, it is just that where searches are a fact of life it becomes difficult to maintain the sorts of activities that constitute everyday life. Seeing privacy as only a matter of the protection of information fails to see the role of lived spaces in everyday life, to see the importance of everyday activity and to recognize the harm done by its intrusions.

This is, of course, part of the larger issue with respect to the no privacy in public rule. It is reinforced by what may be described as the misleading theoretical conception of privacy as intrusion on a person's solitude.[128] It is misleading because it encourages the focus of attention on physical places, but as discussed in Chapter Four, places, whether private or public, become lived spaces, or peopled places, through the people and actions that create them. The law, in privileging private over public categorically, disregards the nature of the activities that occur in peopled places. Thus, attention should be directed away from places that are routinely deemed private or public and instead, should look to the activities and practices that create places and thereby, the ways in which peopled places are supportive of the construction and maintenance of the self and human identity.[129] For example, Anne is walking down the street with her cell phone, which has the ability to track her movements. The telephone beeps and on

---

[127] Gavison, *supra* note 98.

[128] See Chapter Three, Section 2.1, Non-Intrusion" at p 103.

[129] *Ibid.*

the screen is displayed a promotion for a café latte at the Starbucks two blocks away. If Anne is walking from her house to the grocery store to buy food for supper, she is engaging in a private activity, just as if she engages in a political discussion over supper with her family, she is engaging in a public activity. But when Anne walks to the store, what is the status of the place where she is walking. In law, it is a public space. But in a certain way, this is not the important matter. What is important is that these are activities through which people carry on their everyday lives. And they are for this reason, in complex ways, means by which people define their identities. Ultimately, as Helen Nissenbaum asserts, "no matter what principle – actors, spheres, information – is adopted for dividing the world into public and private, it cannot hold ground against a growing host of socio-technical systems in which radically expanded powers over information have been implemented. Because of these powers, there are no actors, no spheres, no information that can be assigned unconditionally to the domain of the public, free of all and any constraints imposed by rights of privacy; none are 'up for grabs.'"[130]

4. Conclusion

The central goal of this dissertation has been to find a new conceptual basis upon which to sustain effective legal protection of spatial privacy. The essence of this chapter has been to build and apply a new construct of "peopled places" to address the deficiencies of the current territorial model of privacy. This construction and application was informed by the work of Chapter Four, which examined the meaning of place. Ultimately, an experiential conception of place, as developed within phenomenological and humanistic geography, was adopted. By promulgating an approach that demands spaces to be understood not as empty vessels but as peopled places, this chapter has affirmed the Supreme Court of Canada's long standing

[130] Nissenbaum, *supra* note 24 at 126.

intention to remedy the trespass theory of privacy by linking section 8 of the *Charter* to the protection of "people, not places".

While there remains in the literature, a persistent tendency to discuss spatial privacy by reference to the panopticon and Big Brother, as discussed in Chapter Two, this no longer holds the metaphorical value it once did. Indeed, this type of ideology actually serves to reinforce the inadequacy of the current territorial model of spatial privacy because the panopticon analysis sees "space as a container."[131] When space or place functions as a container, it fails to capture the dimensions and practices that characterize, and are critical to, contemporary life and everyday interactions. The "containerization"[132] of space makes it difficult, in law, to give effect to the privacy expectations we have in the broader spatiality in which we increasingly live. Peopled places enables a richer understanding of the scope of privacy interests that transcend container thinking by building a concept of place around four defining features: embodiment, contextual dimensions, mobile interactions and boundary management. This construct takes into account the extent to which pervasive computing shapes the ways we experience and live in the world. Law, in turn, has a more effective basis to assess spatial privacy.

This chapter concludes, as it began, with Ludwig Wittgenstein. One constructs the world, Wittgenstein asserts against the background of "the whole hurly-burly of human actions…[s]eeing life as a weave, this pattern is not always complete and is varied in a multiplicity of ways…And one pattern in the weave is interwoven with many others."[133] For Wittgenstein then, we are not isolated individuals in absolute space, but rather actors within the weave, the hurly-burly of life. The metaphor of the weave functions to point attention to the interconnectedness of people's actions. At the heart of Wittgenstein's assertion is an appreciation of the nature of places and their role in everyday lives in which those places are not carved out of a pre-existing

---

[131] Hille Koskela, "The Gaze Without Eyes: Video Surveillance and the Changing Nature of Urban Space" (2000) 24 Progress in Human Geography 243, 250; see also David Lyon, *The Electronic Eye: The Rise of the Surveillance Society* (Minneapolis: Univ. of Minn. Press, 1994) Chapter Four, at 57.

[132] Koskela, *ibid*.

[133] Ludwig Wittgenstein, *Zettel*, trans by GEM Anscombe & Georg H Von Wright (Oxford: Blackwell, 1967) 567.

container, but are created and maintained through our everyday actions of everyday life. Mark Weiser saw this too when he articulated his vision for ubiquitous computing as weaving into the fabric of everyday life. In this dissertation, the peopled places construct was proposed as a means of better understanding this weave, providing ultimately a deeper basis for the development of a theory of spatial privacy in the face of ubiquitous computing.

CONCLUSION

> *There is nothing inevitable about the erosion of privacy, just as there is nothing inevitable about its reconstruction. We have the ability to rebuild private spaces we have lost. But do we have the will?*
>
> Jeffrey Rosen, *The Unwanted Gaze,* (2000)

In April 2013, a sharp plunge in global shipments of personal computers was recorded after a year of increasingly bad news for the PC market. According to reports, the ailing personal computer market is getting weaker and it may not recover as a new generation of mobile devices "reshapes the way people use technology." [1] This headline suggests we may be moving yet closer again to Mark Weiser's vision, as first set out in the Introduction to this dissertation, of redefining the entire relationship of humans and technology for the post-PC era where each person would interact with many 'computers' in their daily lives. A diverse range of technologies are operating beyond what many of us accepted as the traditional site of computing – the desktop or laptop PC. The things in our lives are becoming 'smart'; our phones, our appliances, our running shoes, our cars. We are getting accustomed to finding advanced technology in places that would otherwise have been unlikely even just a few years ago.

Nicholas Carr suggests that the advent of the electrical grid some two hundred years ago offers parallels for understanding the potential implications of this next technological revolution we are currently experiencing.[2] Carr argues that while the grid was originally developed primarily as a means to provide safe and accessible power to industry, it set off a chain reaction of unanticipated effects that ultimately transformed North American society. In the realm of buildings and cities, these ranged

---

1 Michael Liedtke & Peter Svensson, "Personal computer sales decline steeply" The Spokesman-Review: Business (11 April 2013): online: The Spokesman-Review <http://www.spokesman.com/stories/2013/apr/11/personal-computer-sales-decline-steeply/>.

2 Nicholas Carr, *The Big Switch: Rewiring the World from Edison to Google*, (New York: W.W. Norton & Co., 2008).

from the proliferation of artificial lighting that opened up cities to new forms of outdoor nightlife, to the provision of power for the elevators that enabled buildings to grow taller and the machines that displaced craft workers from their roles in production and fabrication. Carr further contends that the electrical grid fostered even more profound and long-lasting changes, as for example, "[t]he rise of the middle class, the expansion of public education, the flowering of mass culture, the movement of the population to the suburbs, the shift from an industrial to a service economy."[3] None of which, Carr argues, "would have happened without cheap current generated by utilities," yet all of which, in turn, were reflected in transformations in the built environment.[4]

The ubiquitous computing paradigm is a similarly fundamental reconfiguration of physical space. In Chapter One, the next generation of computing was examined; from home to work, to school, to restaurants, to shops and roads, in which a vast and mostly invisible layer of technology is being embedded into the world around us and everyday devices. Using a wide range of complex enabling technologies, from microprocessors and RFIDs to sensors to networked information systems, our lived spaces are being transformed, imbued with the capacity to sense, observe, record, process, transmit and respond to information and activity taking place within and around them. All of which reflect the three key characteristics of ubiquitous computing; physicality, invisibility and context-awareness. These key characteristics served as the foundation for reasserting and examining the central focus of this dissertation, spatial privacy.

First, physicality, because computing is brought back into the real world, spread throughout the environment, seamlessly integrated into all facets of our daily lives. Rather than people living most of their lives online, ubiquitous computing replaces the disembodied nature of cyberspace with natural interfaces with and in the physical world. Thus, the relationship between embodied action and meaning, the source of which is not a collection of abstract entities, but rather found in the world in which we

---

[3] *Ibid* at 24.

[4] *Ibid*.

act and experience. Moreover, ubicomp moves away from the separation of information transmission from the physical means of transportation, to re-embedding information and communication technologies into mobile and pervasive environments. Since information can be actively distributed and processed, the self is distributed throughout a ubiquitous computing network and across the lived spaces of everyday life. Second, the invisibility characteristic of ubicomp describes computing receding into the background, where a device is literally or physically visible, but effectively invisible. This notion of disappearance builds on Martin Heidegger's invisibility in use analysis, and Marshall McLuhan's invisible infrastructure model. Weiser drew from these theories to propose the disappearing interface, or what he called 'calm computing,' technology that moves between the periphery and the centre of attention. The ultimate goal, not unlike writing or electricity, was that computing would become commonplace, disappearing behind the scenes into task-specific devices that maintain all the power without the difficulties. And finally, context-awareness is the third key characteristic of ubiquitous computing. The ubiquitous computing paradigm relies on computers being able to sense their surroundings and being able to communicate with other computational objects. By examining and reacting to a user's context to promote and mediate people's interactions with each other, and their environment, context-awareness focuses on detecting, identifying and locating people's movements, routines and actions.

What emerged from the convergence of these characteristics was the focus of Chapter Two: the unique ability and enhanced capabilities for new surveillance practices, locating, monitoring and tracking people and things anywhere, anytime. As a result, data capture will certainly reach new levels, but now too, the spatial dimensions of our everyday lives are more directly and more pervasively compromised and the privacy expectations that accompany them. Traditionally, the observation and monitoring of individuals were attained through the physical, direct viewing of people, their behaviours and the places in which the activities occurred, as demonstrated by Foucault's panoptic prison gaze. However, as David Lyon has argued, with the rise of information and communication technologies, surveillance has extended into other

domains, becoming more intensive and extensive, yet less obtrusive.[5] It is now a form of mediated visibility and exposure stretched across lived spaces. For Kevin Haggerty and Richard Ericson, historical formulations of privacy "overlook the vital point that new surveillance practices have produced important qualitative changes in the experience of privacy."[6] What remains, however, is a focus on the data protection model of informational privacy, largely ignoring the spatial dimensions of privacy. Ubicomp, and the surveillance practices that it facilitates, necessitates revisiting spatial privacy to ensure these interests are adequately protected.

In Chapter Three, the conceptual and legal foundations of privacy were canvassed with a view to determining what spatial privacy is and to what extent it is protected in law, specifically as it has been developed under section 8 of the *Charter*. Although three categories of privacy interests have been recognized, the zonal approach in itself is problematic because it does not take into account cases where there are overlapping privacy interests which risks spatial privacy interests being collapsed into the informational paradigm. This is compounded because the dominant analytical approach employed by the Supreme Court of Canada has been to assess section 8 privacy claims on an informational basis. Applying the narrow interpretation of personal information as 'core biographical information' diminishes the protection of other privacy interests, namely spatial privacy. And finally, central to this dissertation, the current legal construct for spatial privacy remains entrenched in its territorial roots despite the pronouncement that privacy protects people, not places. As a result, the current construct cannot adequately accommodate the changing nature of technologies. What is needed, therefore, is a new conceptual construct of territorial privacy that can be used to sustain effective legal protection of the spatial interests implicated by ubicomp surveillance. This dissertation proposed 'peopled places' to better reflect the spatiality of our lives.

---

[5] David Lyon, *Surveillance Studies: An Overview*, (Cambridge, UK: Polity Press, 2007).

[6] Kevin Haggerty and Richard Ericson, "The New Politics of Surveillance and Visibility" in Haggerty & Ericson, eds, *The New Politics of Surveillance and Visibility* (Toronto, ON: University of Toronto Press, 2006) at 11.

To begin the building process, Chapter Four investigated the meaning of place in order to ground a new conceptual construct of peopled places in an understanding of place that was not tied exclusively to its traditional geographic roots. Place should be seen as less about an absolute location, a spot on the map, and more about the meaningful connections with the many sites in our lives. Grounding life in effective contexts remains absolutely necessary, but this means a conception of place that encompasses all the dimensions of our lived experiences. Moreover, although the concept of 'place' is complex, we need to be concerned with the predominant discourse on data protection because this focus, in the process, fails to see the role of places in everyday life. All too often, the application of the data-protection approach fails to take into account the importance of our everyday activity, no matter how mundane, and in doing so, not recognizing the damage done by its disruption.

Place is not just the 'where' of something. In any given place we encounter a combination of physicality *and* meaning. For Humanists', a place's texture "calls attention to the paradoxical nature of place. Although we may think of texture as a superficial layer, only 'skin deep,' its distinctive qualities may be profound. A surface is, after all, where subject and object merge; the shape, feel and texture of a place each provides a glimpse into the processes, structures, spaces and histories that went into its making."[7] Understanding place in this way highlights the weaving together of the material world, social relations, human-computer interaction and the meaning attributed to place by people as a result. An experiential understanding of place overcomes the extent to which law is currently constrained by its reliance on traditional geography and property concepts.

Based on this understanding of place, the conceptual construct of peopled places was developed in Chapter Five around four defining features: embodiment of place, contextual dimensions, mobility and boundaries. First, we may think of space as abstract and non-physical, yet 'lived spaces' or place, are in fact very much physical. We cannot escape spatiality. We are spatial beings who live and interact with other people

---

[7] Paul Adams, Steven Hoelscher and Karen Till, "Place in Context" in Adams, Hoelscher & Till, eds, *Textures of Place: Exploring Humanist Geographies*, (Minneapolis: University of Minnesota Press, 2001) at xiii.

and physical things in the world. Because we are spatial beings, our body is the central reference point for inhabiting real space and by doing so it becomes place as we appropriate it, interpret it and give it meaning. Second, the contextual dimensions developed in Chapter Five move beyond the more rigid legal contextual analysis used by the courts that position spatial privacy interests either insider or outside traditional private spaces. The place itself may simply be seen as a spatial location, but the relationship between people and places is far richer and more complex than that, encompassing people's actions, activities, practice, interactions and experience. Peopled places captures this complexity by acknowledging important aspects of our personal and practical lives and by taking into account the broader physical and social contexts. Third, the use of mobile and location-aware technologies transforms our experience of places and spaces. The peopled places construct is not dependent on fixed spatial boundaries, but rather, recognizes the flows and connectedness in which we move. In this way, place is not defined by Cartesian measurements or containment, but instead by distributing and the weaving together of social, human and physical interactions. Finally, building Irwin Altman's boundary management theory of privacy forms part of peopled places as a means to move away from the exclusionary and containment formulations of privacy that serve to constrain legal protections.

Chapter Five concludes by providing legal examples to illustrate how the peopled places construct will better accommodate privacy interests in an environment of ubiquitous computing. By promulgating an approach that demands spaces to be understood not as empty vessels but as peopled places, this dissertation affirms, clarifies and elaborates the Supreme Court of Canada's long standing intention to remedy the trespass theory of privacy by linking section 8 of the *Charter* to the protection of "people, not places." Ultimately, as this dissertation has claimed, if privacy is to protect people, it must protect them in their lived embodied spaces.

The construct of peopled places derived in this dissertation contributes to privacy scholarship and law by offering a conceptual basis for sustaining adequate legal protection of spatial privacy interests. Its first iteration in this dissertation is not intended as fully comprehensive in answering all the plaguing privacy questions that

are certain to arise. Future work will build on this foundation to address, for example: (i) the extent to which state interests in providing greater security and enhanced law enforcement techniques to detect crimes will prevail over spatial privacy interests implicated by those practices; (ii) the development of a constitutional test that takes into account the changing nature of technology and surveillance practices; and (iii) building a boundary management theory that effectively responds to technology-mediated interactions that implicate both the informational *and* spatial dimensions of privacy. Some of this work is already being done in the American context.[8] This dissertation has sought to entrench the crucial anchor points for future Canadian analysis.

To conclude, over twenty years ago, Mark Weiser predicted the next generation of computing would activate the world. Rich Gold analogized ubiquitous computing as computers talking like "chattering animals in a living jungle, sometimes exchanging detailed information, sometimes just noting who is around."[9] In May 2013, Wired Magazine proclaimed "Awake" to describe when objects around us talk to one another, the elements of the physical universe converge and "spring to life."[10] Soon, according to Bill Wasik, "we'll be able to choreograph them to respond to our needs, solve our problems, even save our lives."[11] Intelligence once locked in devices or behind physical barriers can now flow into the world of physical objects, but "the true genius" of smart things is having a "grid of bubbles that show the status of people and places and things on your system and the various programs that connect them."[12] Will the privacy concerns of a sensor-connected world be, as Waslik suggests, "fast outweighed by the

---

8 See for example, Julie Cohen, Reconfiguring the Networked Self: Law, Code and the Play of Everyday Practice, (New Haven, CT: Yale University Press, 2012); Daniel Solove, "Fourth Amendment Pragmatism" (2010), online: <http://www.bc.edu/content/dam/files/schools/law/bclawreview/pdf/51_5/04_solove.pdf>; and Orin Kerr, "An Equilibrium Adjustment Theory of the Fourth Amendment" (2011) 125 Harvard Law Review 476-543.

9 Rich Gold, "This is Not a Pipe" (1993) 36:7 ACM 72.

10 Bill Wasik, "Welcome to the Programmable World" *Wired* Magazine (May 2013) 140.

11 *Ibid*.

12 *Ibid* at 147.

strange pleasures of residing in it"? Or, as Jeffrey Rosen implies in the quotation at the outset of this conclusion, will we re-build private spaces to comport with existing norms and values?

BIBLIOGRAPHY

Legislation

Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11, s 8.

Civil Code of Quebéc, SQ 1991, c 64.

Combines Investigation Act, RSC 1970, c C-23.

Quebec Charter of Human Rights and Freedoms, RSQ 1975, c C-12, s 5.

US Constitution, Amendment IV.

Jurisprudence

Aubry v Éditions Vice-Versa Inc. [1998] 1 SCR 591.

Dagg v Canada (Minister of Finance) [1997] 2 SCR 403.

Griswold v Connecticut (1965), 381 US 479.

Hunter v Southam Inc., [1984] 2 SCR 145.

Katz v United States (1967), 389 US 347.

Kyllo v United States (2001), 533 US 27.

R v AM [2006] OJ 1663.

R v Belnavis [1997] 3 SCR 341.

R v Briggs (2001) 157 CCC (3d) 38 (OntCA).

R v Buhay [2003] 1 SCR 631.

R v *Chetwynd* (1996) 161 NSR (2d) 391 (SC).

R v Colarusso [1994] 1 SCR 20.

R v Collins [1987] 1 SCR 265.

R v Duarte [1990] 1 SCR 30.

R v Dyment [1988] 2 SCR 417.

R v Edwards [1996] 1 SCR 128.

R v Evans, [1996] 1 SCR 8.

R v Feeney [1997] 2 SCR 13.

R v Gomboc, [2010] 2 SCR 211.

R v Greffe [1990] 1 SCR 755.

R v Harrison, [2009] 2 SCR 494

R v Kang-Brown, [2008] 1 SCR 456.

R v *Kokesch* [1990] 3 SCR 3.

R v Laurin (1997), 98 OAC 50.

R v Law [2002] 1 SCR 227.

R v LeBeau (1988), 25 OAC 1 (CA).

R v M (MR) [1998] 3 SCR 393.

R v Nolan, [1987] 1 SCR 1212.

R v Nolet [2010] 1 SCR 851 (SCC).

R v *Mellenthin* [1992] 3 SCR 615.

R v O'Flaherty (1987), 63 Nfld. & PEIR 21 (Nfld. CA).

R v Osanyinlusi, [2006] OJ 2529 (QL) (ON SCJ).

R v Patrick [2009] 1 SCR 579.

R v Plant [1993] 3 SCR 281.

R v Pohoretsky [1987] 1 SCR 945

R v Pugliese (1992), 52 OAC 280.

R v Ritter 2006 ABPC 162, 402 AR 249.

R v SAB [2003] 2 SCR 678.

R v Silva (1995), 26 OR (3d) 554 (Gen Div).

R v Silveira [1998] 2 SCR 297.

R v Simmons [1988] 2 SCR 495.

R v Simpson [2005] OJ 5056 (QL) (ON SCJ).

R v Stillman [1997] 1 SCR 607.

R v Telus Communciations Company (2013), SCC 16, [2013] SCJ 16 (QL).

R v Tessling (2003) 63 OR (3d) 1 (CA).

R v Tessling [2004] 3 SCR 432.

R v Wise [1992] 1 SCR 527.

R v Wong [1990] 3 SCR 36.

Semayne v Gresham (1604), 77 ER 194 (KB).

The People of the State of California v Scott Lee Peterson, Superior Court of the State of California for the County of Stanislaus, Case No. 1056770.

United States v Jones (2012) 565 US 132 S Ct. 945.

Secondary Material: Books

Aarts, Emile & José Encarnação, eds. *True Visions: The Emergence of Ambient Intelligence* (Berlin: Springer, 2006).

Aarts, Emile & Stefano Marzano. *The New Everyday: View of Ambient Intelligence* (Rotterdam: 010 Publishers, 2003).

Agnew John. “Space: Place” in Paul Cloke & Ron Johnston, eds. *Spaces of Geographical Thought* (London: Sage, 2003) 81.

Agnew, John. *Place and Politics* (Boston, MA: Allen & Unwin, 1987).

Ahonen, Pasi et al. “From Ubiquitous Computing to Ambient Intelligence” in David Wright et al, eds. *Safeguards in a World of Ambient Intelligence* (Berlin: Springer, 2008) 1, online: <http://www.springer.com/computer/database+management+%26+information+retrieval/book/978-1-4020-6661-0>.

Alahuhta, Petteri et al. “Dark Scenarios in Ambient Intelligence: Highlighting Risks and Vulnerabilities (SWAMI Deliverable D2)” in David Wright et al, eds. *Safeguards in a World of Ambient Intelligence (SWAMI)* (2006) at 6, Online: <http://www.springer.com/computer/database+management+%26+information+retrieval/book/978-1-4020-6661-0>

Alexander, Christopher. *The Timeless Way of Building* (Oxford, UK: Oxford University Press, 1979).

Algra, Keimpe. *Concepts of Space in Greek Thought* (Leiden, Netherlands: Brill, 1995).

Allen, Anita L. *Uneasy Access: Privacy for Women in a Free Society* (Totowa, NJ: Rowman & Littlefield, 1988).

Allen, Anita. *Unpopular Privacy* (New York: Oxford University Press, 2011).

Altman, Irwin & Setha M Low, eds. *Human Behavior and Environments: Advances in theory and research, vol 12: Place Attachment* (New York: Plenium Press, 1992).

Altman, Irwin. *The Environment and Social Behaviour: Privacy, Personal Space, Territory and Crowding* (Monterey, CA: Brooks/Cole, 1975)

Andrejevic, Mark. *iSpy: Surveillance and Power in the Interactive Era* (Lawrence, KS: University of Kansas Press, 2004).

Arendt, Hannah. *The Human Condition* (Chicago: University of Chicago Press, 1958).

Augé, Marc. *Non-Places: Introduction to an Anthropology of Supermodernity* (New York: Verso, 1995).

Augusto, Juan Carlos & Daniel Shapiro. *Advances in Ambient Intelligence* (Amsterdam: IOS Press, 2007).

Bachelard, Gaston. *The Poetics of Space: The Classic Look at How We Experience Intimate Places*, translated by Maria Jolas (New York: Orion Press, 1964).

Ball, Kirsty, Kevin Haggerty & David Lyon. *Routledge Handbook of Surveillance Studies* (New York: Routledge, 2012).

Barkhaus, Louise & Paul Dourish. "Everyday Encounters with Context-Aware Computing in the Campus Environment" in *Proceedings of the International Conference on Ubiquitous Computing* (Nottingham, UK: Springer, 2004) 232.

Bennett, Colin & Lori Crowe, "Location-Based Services and the Surveillance of Mobility: An Analysis of Privacy Risks in Canada," in *Report to the Office of the Privacy Commissioner of Canada* (June 2005).

Bennett, Colin. *Privacy Advocates: Resisting the Spread of Surveillance* (Cambridge, MA: MIT Press, 2008).

Bergum, Vangie. "Being a Phenomenological Researcher" in Janice M Morse, ed. *Qualitative nursing research: A contemporary dialogue* (Newbury Park, CA: Sage, 1991) 55.

Bilandzic, Mark. "The Embodied Hybrid Space: Designing Ubiquitous Computing Towards an Amplification of Situated Real World Experiences" in *Proceedings of OZCHI* (New York: ACM, 2010) 422.

Bok, Sissela. *Secrets: On the Ethics of Concealment and Revelation* (New York: Random House, 1989).

Brin, David. *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* (Cambridge, MA: Perseus Books, 1998).

Buxton, William. "Less is More (More or Less)" in Paul Denning, ed. *The Invisible Future: The Seamless Integration of Technology in Everyday Life* (NY: McGraw-Hill, 2001) 145.

Cai, Yang & Julio Abascal, eds. *Ambient Intelligence in Everyday Life* (Berlin: Springer, 2006).

Calo, M Ryan. "Robots and Privacy" in Patrick Lin et al, eds. *Robot Ethics: The Ethical & Social Implications of Robotics* (Cambridge, MA: MIT Press, 2012) Chapter 12, 187.

Canter, David. "The Facets of Place" in Gary T Moore & Robert W Marans, eds. *Advances in Environment, Behaviour and Design* (New York: Plenum, 1997) 109.

Carrol, Lewis. *Alice's Adventures in Wonderland and Through the Looking Glass* (London: Puffin Books, 1996).

Casey, Edward. *Getting Back into Place* (Bloomington, ID: Indiana University Press, 1994).

Casey, Edward. *The Fate of Place: A Philosophical History* (Berkeley, CA: University of California Press, 1997).

Castells, Manuel. *The Rise of the Network Society* (Oxford: Blackwell, 1996) at 376.

Cawood, Stephen & Mark Fiala. *Augmented Reality: A Practical Guide* (Raleigh, NC: Pragmatic Bookshelf, 2008).

Chandler, Jennifer. "Privacy Versus National Security: Clarifying the Trade-Off" in Ian Kerr, Valerie Steeves & Carole Lucock, eds. *Lessons From the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Toronto: Oxford University Press, 2009) 121.

Cohen, Julie. *Configuring the Networked Self: Law, Code and the Play of Everyday Practice* (New Haven, CT: Yale University Press, 2012).

Cooley, Thomas M *A Treatise on the Law of Torts or the Wrongs which Arise Independent of Contract*, 2nd ed (Chicago: Callaghan & Co, 1888).

Crabtree, Noel. "Place: Connections and Boundaries in an Independent World" in Nicholas Clifford et al, eds. *Key Concepts in Geography*, (London: Sage Publications, 2009) 153-171.

Cresswell, Tim. *On The Move: The Politics of Mobility in the Modern West* (London: Routledge, 2006).

Cresswell, Tim. *Place: A Short Introduction* (Oxford, UK: Blackwell, 2004).

Curry, Michael R. "Hereness and the Normativity of Places" in James D Proctor & David M Smith, eds. *Geography and Ethics* (London: Routledge, 1999) 95.

Curry, Michael. "Discursive Displacement and the Seminal Ambiguity of Space and Place" in Leah Lievrouw & Sonia Livingstone, eds. *The Handbook of New Media* (London: Sage Publications, 2002) 503.

de Certeau, Michel. *The Practice of Everyday Life*, translated by Steven Rendall (Berkeley, CA, University of California Press, 1984).

de Souza e Silva, Adriana & Daniel M Sutko. "An Interview With Matt Adams from Blast Theory" in Adriana de Souza e Silva & Daniel M Sutko, eds. *Digital Cityscapes* (New York: Peter Lang, 2009) 71.

DeCew, Judith Wagner. *In Pursuit of Privacy: Law, Ethics and the Rise of Technology* (Ithaca: Cornell University Press, 1997).

Denning, Peter J, ed. *The Invisible Future: The Seamless Integration of Technology into Everyday Life* (New York: McGraw-Hill, 2002).

Dickens, Charles. *A Tale of Two Cities* (London: Penguin Books, 2000).

Dourish, Paul. *Where the Action Is: The Foundations of Embodied Interaction* (Cambridge, MA: MIT Press, 2001).

Duncan, James. "Place" in Ron Johnston et al, eds. *The Dictionary of Human Geography* (Oxford, UK: Blackwell, 2000).

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

Einstein, Albert, in Max Jammer. *The Concepts of Space in Physics*, 3rd ed (Toronto, ON: General, 1993).

Embree, Lester. *The Encyclopedia of Phenomenology* (Dordrecht, The Netherlands: Kluwer, 1996).

Entrikin, J Nicholas. *The Betweenness of Place: Towards a Geography of Modernity* (Baltimore, MD: John Hopkins University Press, 1991).

Fouberg, Erin & Alexander B Murphy. *Human Geography: People, Place and Culture* (Hoboken, NJ: Wiley & Sons, 2009).

Foucault, Michel. *Discipline & Punish: the Birth of the Prison*, translated by Alan Sheridan (New York: Random House, 1995).

Fox, Michael & Miles Kemp, *Interactive Architecture* (New York: Princeton Architectural Press, 2010).

Friedberg, Anne. "The Mobilized and the Virtual Gaze in Modernity" in Nicholas Mirzoeff. *The Visual Culture Reader* (New York: Routledge, 2002) 395.

Gabler, Neil. *Walt Disney: The Triumph of the American Imagination* (New York: Random House, 2006).

Gallager, Shawn & Dan Zahavi, eds. *Phenomenology and the Cognitive Science* (New York: Springer, 2010).

Gandy, Oscar. *The Panoptic Sort: A Political Economy of Personal Information* (Boulder, CO: Westview Press, 1993).

Garfinkel, Simson & Beth Rosenberg, eds. *RFID: Applications, Security and Privacy* (Boston, MA: Addison-Wesley, 2006).

Garfinkel, Simson. *Database Nation: The Death of Privacy in the 21st Century* (Sebastopol, CA: O'Reilly & Associates, 2000).

Gates, Bill. *Business at the Speed of Thought: Using a Digital Nervous System* (New York: Warner Books, 1999).

Gershenfeld, Neil. *When Things Start to Think* (New York: Henry Holt & Co, 1999).

Gibson, JJ. *The Ecological Approach to Visual Perception* (New York: Houghton-Mifflin, 1979).

Gibson, William. *Burning Chrome* (New York, NY: Harper Collins, 1986).

Gibson, William. *Neuromancer* (New York: Ace Books, 1984).

Gifford, Robert. *Environmental Psychology: Principles and Practice* (Coleville, WA: Optimal Books, 2007).

Gilliom. John"Struggling with Surveillance: Resistance, Consciousness and Identity" in Kevin D Haggerty & Richard V Ericson. *The New Politics of Surveillance and Visibility* (Toronto, ON: University of Toronto Press, 2006) 111.

Goffman, Erving. *Behaviour in Public Places* (NY: Free Press, 1963).

Goffman, Erving. "The Territories of the Self" in *Relations in Public: Microstudies of the Public Order* (New York: Basic Books, 1979) 38.

Goffman, Erving. *The Presentation of Self in Everyday Life* (Garden City, NY: Doubleday, 1959).

Gow, Gordon & Richard Smith. *Mobile & Wireless* (UK: Open University Press, 2006).

Graham, Stephen. "Excavating the Material Geographies of Cyber-cities" in Stephen Graham, ed. *The Cyber-cities Reader* (London: Routledge, 2003) 139.

Green, Nicola. "Who's Watching Whom: Monitoring and Accountability in Mobile Relations" in Barry Brown, Nicola Green & Richard Harper, eds. *Wireless World: Social and Interactional Aspects of the Mobile Age* (London: Springer, 2002) 32.

Greene, Brian. *The Fabric of the Cosmos: Space, Time and the Texture of Reality* (New York: Vintage Books, 2004).

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

Guelke, Leonard. *Historical Understandings in Geography: An Idealist Approach* (Cambridge, UK: Cambridge University Press, 1982).

Habermas, Jurgen. *The Structural Transformation of the Public Sphere* (Cambridge, MA: MIT Press, 1989).

Haggerty, Kevin D & Richard V Ericson, "The New Politics of Surveillance and Visibility" in Kevin D Haggerty & Richard V Ericson. *The New Politics of Surveillance and Visibility* (Toronto, ON: University of Toronto Press, 2006) 4.

Haggerty, Kevin D "Tear Down the Walls: On Demolishing the Panopticon" in David Lyon, ed. *Theorizing Surveillance: The Panopticon and Beyond* (Portland, OR: Willan, 2006) 38.

Hainich, Rolf. *The End of Hardware: A Novel Approach to Augmented Reality*, 3rd ed (Charleston, SC: Booksurge, 2006).

Hall, ET. *The Hidden Dimension* (Garden City, NY: Doubleday, 1966).

Hall, Edward T. *The Silent Language* (New York: Doubleday, 1959).

Harper, Richard, ed. *Inside the Smart Home* (London: Springer, 2003).

Harvey, David. "From Space to Place and Back Again" in Jon Bird et al, eds. *Mapping the Futures: Local Cultures, Global Change* (London: Routledge, 1993) 3.

Harvey, David. *Justice, Nature and the Geography of Difference* (Cambridge, MA: Blackwell, 1987).

Heidegger, Martin. *Being and Time*, translated by Joan Stambaugh (Albany, NY: State University of New York Press, 1996).

Hier, Sean & Josh Greenberg, eds. *The Surveillance Studies Reader* (Maidenhead, England: Open University Press, 2007).

Holder, Jane & Carolyn Harrison, eds. *Law and Geography* (Oxford, UK: Oxford University Press, 2003).

Holzinger, Andreas & Klaus Miesenberger, eds. *HCI and Usability for e-Inclusion* (Berlin: Springer, 2009).

Hooks, Bell. "Homeplace: a site of resistance" in *Yearning: Race, Gender, and Cultural Politics* (Boston: South End Press, 1991).

Huggett, Nick. *Space From Zeno to Einstein: Classic Readings with a Contemporary Reading* (Cambridge, MA: MIT Press, 1999).

Husserl, Edmund. *Ideas: General Introduction to Pure Phenomenology,* translated by W R Boyce Gibson (New York: Routledge, 2012).

Igoe, Tom & Dan O'Sullivan. *Physical Computing: Sensing and Controlling the Physical World with Computers* (Boston: Thomson Course Technology, 2004).

Inness, Julie. *Privacy, Intimacy and Isolation* (New York: Oxford University Press, 1992).

Ishii, Hiroshi. "Tangible Bits: Coupling Physicality and Virtuality Through Tangible User Interfaces" in Yuichi Ohta & Hideyuki Tamura, eds. *Mixed Reality: Merging Real and Virtual Worlds* (New York: Springer, 1999) 41.

Jacobs, Jane. *The Death and Life of Great American Cities* (New York: Vintage Books, 1992).

Jain, Anil K, Ruud M Bolle & Sharath Pankanti, eds. *Biometrics: Personal Identification in the Networked Society* (London: Springer, 2003).

Jenkins, Henry. *Convergence Culture* (New York: New York University Press, 2005).

Kerr, Ian, Jennifer Barrigar, Jacquelyn Burkell & Katie Black. "Soft Surveillance, Hard Consent: The Law and Psychology of Engineering Consent" in Ian Kerr, Valerie Steeves & Carole Lucock, eds. *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked* Society (Toronto, ON: Oxford University Press, 2009) 5.

Kerr, Ian. "The Internet of People: Reflections on the Future Regulation of Human-Implantable Radio-Frequency Identification" in Ian Kerr, Valerie Steeves & Carole Lucock, eds. *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked* Society (Toronto, ON: Oxford University Press, 2009) 335.

Klapp, Orrin. *Overload and Boredom: Essays in the Quality of Life in the Information Society* (New York, Greenwood Press, 1986).

Kockelmans, Joseph J. *Phenomenology and Physical Science* (Pittsburg, PA: Duquesne University Press, 1966).

Kostakos, Vassilis et al. "Design Tools for Pervasive Computing in Urban Environments" in *Proceedings 8th International Conference on Design and Decision Support Systems in Archictecture and Urban Planning* (Netherlands: Springer, 2006) 467.

Krasniewicz, Louise & Michael Blitz. *Walt Disney: A Biography* (Santa Barbara, CA: Greenwood, 2010).

Kuniavsky, Mike. *Smart Things: Ubiquitous Computing User Design Experience* (Burlington, MA: Elsevier, 2010).

Kunstler, James. *The Geography of Nowhere* (New York: Touchstone, 1993).

Lefebvre, Henri. *The Production of Space*, translated by Donald Nicholson Smith (Malden, MA: Blackwell, 1991).

Levinson, Paul. *Cellphone: The Story of the Most Mobile Medium and How it Transformed Everything* (New York: Palgrave MacMillan, 2004).

Luijpen, William. *Phenomenology and Humanism* (Pittsburg, PA: Duquesne University Press, 1996).

Lyon, David, ed. *Theorizing Surveillance: The Panopticon and Beyond* (Portland, OR: Willan, 2006).

Lyon, David. "Chapter 5: Security, Suspicion, Social Sorting" in *Surveillance Studies: An Overview* (Cambridge: Polity, 2007) 94.

Lyon, David. *Identifying Citizens: ID Cards as Surveillance* (Oxford: Polity Press, 2009).

Lyon, David. *Surveillance After September 11* (Cambridge: Polity, 2003).

Lyon, David. *Surveillance Society: Monitoring Everyday Life* (Buckingham, UK: Open University Press, 2001).

Lyon, David. *The Electronic Eye: The Rise of the Surveillance Society* (Cambridge: Polity, 1994).

MacKinnon, Catharine A. *Feminism Unmodified: Discourses on Life and Law* (Cambridge, MA: Harvard University Press, 1987).

MacKinnon, Catherine. *Toward A Feminist Theory of the State* (Cambridge, MA: Harvard University Press, 1989).

Malpas, Jeff. *Heidegger's Topology: Being, Place, World* (Cambridge, MA: MIT Press, 2006).

Malpas, Jeff. *Place and Experience: A Philosophical Topography* (Cambridge, UK: Cambridge University Press, 1999).

Martin, Geoffrey. *All Possible Worlds: A History of Geographic Ideas*, 4th ed (New York: Oxford University Press, 2005).

Marx, Gary. "Soft Surveillance: The Growth of Mandatory Volunteerism in the Collection of Personal Information – "Hey Buddy Can you Spare a DNA?"" in Torin Monahan, ed. *Surveillance and Security: Politics and Power in Everyday Life* (London: Routledge, 2007) 47.

Marx, Gary. "Varieties of Personal Information on Influences on Attitudes Towards Surveillance" in Kevin D Haggerty & Richard V Ericson. *The New Politics of Surveillance and Visibility* (Toronto, ON: University of Toronto Press, 2006) 79.

Massey, Doreen & Pat Jess, eds. *A Place in the World? Places, Cultures and Globalization* (Oxford: Oxford University Press, 1995).

Massey, Doreen. "A Global Sense of Place" in T Barnes & D Gregory, eds. *Reading Human Geography*, (London: Arnold, 1997) 315-323.

Massey, Doreen. "Power-geometry and a Progressive Sense of Place" in Jon Bird et al, eds. *Mapping the Futures: Local Cultures, Global Change* (London: Routledge, 1993) 59.

Massey, Doreen. "The Conceptualization of Place" in Doreen Massey & Pat Jess, eds. *A Place in the World? Places, Cultures and Globalization* (Oxford: Oxford University Press, 1995) 45.

Matheson, Dave. "Dignity & Selective Self-Presentation" in Ian Kerr, Valerie Steeves & Carole Lucock, eds. *Lessons from the Identity Trail: Privacy & Identity in a Networked Society* (Toronto, ON: Oxford University Press, 2009) 319;

McCarthy, John & Peter Wright. *Technology as Experience* (Cambridge, MA: MIT Press, 2004).

McCullough, Malcolm. *Digital Ground* (Cambridge, MA: MIT Press, 2005).

McGill, Jena & Ian Kerr. "Reduced to Absurdity: Reasonable Expectations of Privacy and the Need for Digital Enlightenment" in Jacques Bus et al, eds. *Digital Enlightenment Yearbook 2012* (Amsterdam: IOS Press, 2012) 199.

McGill, Jena. "What Have You Done for Me Lately? Reflections on Redeeming Privacy for Battered Women" in Ian Kerr, Valerie Steeves & Carole Lucock, eds. *Lessons from the Identity Trail: Privacy & Identity in a Networked Society* (Toronto, ON: Oxford University Press, 2009) 157.

McKay, Wendy. "Augmented Reality: Linking the Real and Virtual Worlds, a New Paradigm for Interacting with Computers" in Tiziana Catarei et al, eds. *Proceedings of the Working Conference on Advanced Visual Interfaces* (New York: ACM, 1998).

McLuhan, Eric & Frank Zingrone, eds. *Essential McLuhan* (New York: Basic Books, 1995).

McLuhan, Marshall. *Gutenberg Galaxy: The Making of a Topographic Man* (Toronto: University of Toronto Press, 1962).

Merleau-Ponty, Maurice. *The Phenomenology of Perception*, translated by Colin Smith (New York: Routledge Press, 1958).

Merriman, Peter. "Mobility" in Robert Kitchin & Nigel Thrift, eds. *International Encyclopedia of Human Geography* (London: Elsevier, 2009).

Meyrowitz, Joshua. *No Sense of Place: The Implact of Electronic Media on Social Behaviour,* (New York: Oxford University Press, 1985).

Meyrowitz, Joshua. "The Rise of 'Glocality'" in Kristof Nyiri, ed. *A Sense of Place* (Vienna: Passagen Verlag, 2005).

Mill, John Stuart. *On Liberty and Other Essays*, John Gray, ed (Oxford, UK: Oxford University Press, 1991).

Millard, Mark & Firat Soylu. "An Embodied Approach for Engaged Interaction in Ubiquitous Computing" in Julie Jacko, ed, *Human-Computer Interaction: Ambient, Ubiquitous and Intelligent Interaction* (Berlin: Springer, 2009) 464.

Monmonier, Mark. *Spying With Maps: Surveillance Technologies and the Future of Privacy* (Chicago, Ill: University of Chicago Press, 2002).

Moran, Dermot & Timothy Mooney, eds. *The Phenomenology Reader* (New York: Routledge, 2002).

Mostefaoui, Soraya & Zakaria Maamar, eds, *Advances in Ubiquitous Computing: Future Paradigms and Directions* (Hershey, PA: IGI Global, 2008).

Negroponte, Nicholas. *Being Digital* (NY: Random House, 1995).

Nippert-Eng, Christena. *Islands of Privacy* (Chicago: Chicago University Press, 2010).

Nissenbaum, Helen. *Privacy in Context: Technology, Policy & the Integrity of Social Life* (Stanford, CA: Stanford University Press, 2010).

Norman, Donald. *The Design of Everyday Things* (New York: Basic Books, 2002).

Norman, Donald. *The Design of Future Things* (New York: Basic Books, 2007).

Norman, Donald. *The Invisible Computer* (Cambridge, MA: MIT Press, 1998).

Norris, Clive. "From Personal to Digital: CCTV, the Panopticon and the Technological Mediation of Suspicion and Social Control" in David Lyon, ed. *Surveillance and Social Sorting: Privacy Risk and Automated Discrimination* (London: Routledge, 2002) 268.

O'Harrow, Robert Jr. *No Place to Hide: Behind the Scenes of Our Emerging Surveillance Society* (New York: Free Press, 2005).

O'Sullivan, Dan & Tom Igoe. *Physical Computing: Sensing, Controlling the Physical World with Computers* (Boston, MA: Thomson, 2004).

Pateman, Carole. "Feminist Critiques of the Public/Private Dichotomy" in Carole Pateman. *The Disorder of Woman: Democracy, Feminism and Political Theory* (Palo Alto, CA: Stanford University Press, 1989) 118.

Peet, Richard. *Modern Geographical Thought* (Oxford: Blackwell, 1998).

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

Petronio, Sandra. *Boundaries of Privacy: Dialectics of Disclosure* (Albany, NY: State University of New York Press, 2002).

Pijpers, Guus. *Information Overload: Managing Your Data* (Hoboken, NJ: Wiley & Sons, 2010).

Posner, Richard. *The Economics of Justice* (Cambridge, MA: Harvard Univ Press, 1981).

Poster, Mark. *The Second Media Age* (Cambridge: Polity, 1995).

Postman, Neil. *Amusing Ourselves to Death* (New York: Penguin, 2006).

Pottie, Gregory & William Kaiser, *Principles of Embedded Networked System Design* (Cambridge, UK: Cambridge University Press, 2005).

Powers, Bethel Ann & Thomas R Knapp. *A Dictionary of Nursing Theory and Research*, 2nd ed (Thousand Oaks, CA: Sage, 1995).

Proshansky, Harold. *Environmental Psychology: People and his Physical Setting* (Austin, TX: Holt Rinehart, 1976).

Queens University Surveillance Project. "Location Technologies, Mobility, Surveillance & Privacy" (March 2005) in *Report to the Office of the Privacy Commissioner of Canada*.

Quek, Francis. "Embodiment and Multimodality" in *Proceedings of ICMI 2006 International Conference on Multimodal Interfaces* (New York: ACM Press, 2006) 388.

Quigley, Tim. *Procedure in Canadian Criminal Law*, 2nd ed (Carswell: Toronto, 2005).

Regan, Priscilla. *Legislating Privacy* (Chapel Hill: University of North Carolina Press, 1995).

Reichenbach, Hans. *The Philosophy of Space and Time*, translated by Maria Reichenbach, (New York: Dover Publications, 1957).

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

Reiman, Jeffrey. "Privacy, Intimacy and Personhood" in Ferdinand Schoeman, ed. *Philosophical Dimensions of Privacy, An Anthology* (Cambridge, UK: Cambridge University Press, 1984) 300.

Relph, Edward. *Place and Placelessness* (London, UK: Pion, 1976).

Report of the Task Force established by the Department of Communications and Department of Justice: Privacy and Computers (Ottawa: Communication Group, 1972).

Rheingold, Howard. *Smart Mobs: The Next Social Revolution* (Cambridge, MA: Perseus, 2002).

Riva, Giuseppe et al. "Presence 2010: The emergence of Ambient Intelligence" in *Being There: Concepts, Effects and Measurement of User Presence in Synthetic Environments* (Amsterdam: IOS Press, 2003).

Rose, Gillian. *Feminism and Geography: The Limits of Geographical Knowledge* (Cambridge: Polity, 1993).

Rosen, Jeffrey. *The Unwanted Gaze: The Destruction of Privacy in America* (New York: Random House, 2000).

Rossler, Beate. *The Value of Privacy,* translated by RDV Glasgow (Cambridge, UK: Polity Press, 2005).

Rule, James B. "From Mass Society to Perpetual Contact: Models of Communication Technoloiges in Social Context" in James E Katz & Mark Aakhus, eds. *Perpetual Contact: Mobile Communication, Private Talk, Public Performance* (New York: Cambridge University Press, 2002).

Rule, James. *Private Lives, Public Surveillance* (London: Allen Lane, 1973).

Sack, Robert D. *Homo Geographicus* (Baltimore, MD: John Hopkins University Press, 1997).

Sack, Robert. *A Geographical Guide to the Real and the Good* (New York: Routledge, 2003).

Schafer, Arthur. "Privacy: A Philosophical Overview" in D Gibson, ed. *Aspects of Privacy Law: Essays in Honor of John Sharpe* (Toronto, ON: Butterworths, 1980) 1.

Schilit, Bill, Norman Adams & Roy Want. "Context-Aware Computing Applications" in *Workshop on Mobile Computing Systems and Applications* (Santa Cruz, CA: IEEE, 1994) 85.

Seamon, David. *A Geography of the Lifeworld: Movement, rest and encounter* (New York: St. Martin's Press, 1979).

Sewell, Graham & James Barker. "Neither Good, nor Bad, but Dangerous: Surveillance as an Ethical Paradox" in Sean Hier & Josh Greenberg, eds. *The Surveillance Studies Reader* (Maidenhead, England: Open University Press, 2007) at 354-368.

Sheller, Mimi & John Urry, eds. *Mobile Technologies of the City* (London, UK: Routledge, 2006).

Smith, David Marshall. *Moral Geographies: Ethics in a World of Difference* (Edinburg: Edinburg University Press, 2000).

Soerensen, Natascha, C Oestergaard & Birthe Dinesen. "Improving Care of the Elderly with an 'Intelligent Bed'" in M Jordanova & F Lievens, eds. *Global Telemedicine and eHealth Updates: Knowledge Resources,* vol 5, *2012, Luxembourg* (Lucerne, Switzerland: International Society for Telemedicine & eHealth, 2012) 128.

Sohraby, Kazem, Daniel Minoli & Taieb Znati. *Wireless Sensor Networks: Technology, Protocols and Applications* (Hobeken, NJ: John Wiley & Sons, 2007).

Solove, Daniel J. *The Digital Person: Technology and Privacy in the Information Age* (New York: NY Press, 2004).

Solove, Daniel. *Nothing to Hide: The False Tradeoff between Privacy and Security* (New Haven, CT: Yale University Press, 2011).

Solove, Daniel. *The Future of Reputation: Gossip, Rumour, and Privacy on the Internet* (New Haven, CT: Yale University Press, 2007).

Solove, Daniel. *Understanding Privacy* (Cambridge, MA: Harvard University Press, 2008).

Sommer, Robert. *Personal Space: The Behavourial Basis of Design* (Englewood, NJ: Prentice-Hall, 1969).

Song, Xiang. *Seamless Mobility in the Ubiquitous Computing Environment* (Ann Arbor, MI: ProQuest, 2008).

Spiegelberg, Herbert. *The Phenomenological Movement* (The Hague: Martinus Nijhof, 1960).

Staples, William G. *The Culture of Surveillance: Discipline and Social Control in the United States* (New York: St. Martin's Press, 1997).

Staples, William. *Everyday Surveillance: Vigilance and Visibility in Postmodern Life* (Lanham, MD: Rowman & Littlefield, 2000).

Steele, Fritz. *The Sense of Place* (Boston: CBI, 1981).

Steeves, Valerie. "Reclaiming the Social Value of Privacy" in Ian Kerr, Valerie Steeves & Carole Lucock, eds. *Lessons from the Identity Trail: Anonymity, Privacy and*

Identity in a Networked Society (Toronto, ON: Oxford University Press, 2009) 191.

Sterling, Bruce. *Shaping Things* (Cambridge, MA: MIT Press, 2005).

Stewart, David & Algis Mickunas. *Exploring Phenomenology: A Guide to the Field and its Literature* (Athens, Ohio: Ohio University Press, 1990).

Stuart, Don. *Charter Justice in Canadian Criminal Law*, 5th ed (Carswell: Toronto, 2010).

Suchman, Lucy. *Plans and Situated Actions: The Problem of Human-Machine Communication* (Cambridge: Cambridge University Press, 1987).

Sykes, Charles. *The End of Privacy* (New York: St. Martin's Press, 1999).

Thrift, Nigel & Mike Crang, eds. *Thinking Space* (New York: Routledge, 2000).

Toffler, Alvin. *Future Shock* (New York: Random House, 1970).

Tuan, Yi-Fu. *Space & Place: The Perspective of Experience* (Minneapolis: University of Minnesota Press, 1977).

Ullmer, Brygg & Hiroshi Ishii. "Emerging Frameworks for Tangible User Interfaces" in John Carroll, ed. *Human Computer Interaction in the New Millenium* (NY: Addison-Wesley, 2001) 189.

Van Den Haag, Ernest. "On Privacy" in J Roland & JW Chapman, eds, *Nomos XIII: Privacy* (New York: Atherton Press, 1971).

Varela, Francisco, Evan Thompson & Eleanor Rosch. *The Embodied Mind* (Cambridge, MA: MIT Press, 1991).

Verstraete, Ginette & Tim Cresswell, eds. *Mobilizing Place, Placing Mobility: The politics of representation in a globalized world* (Amsterdam: Rodopi, 2002).

Virilo, Paul. *The Vision Machine*, translated by Julie Rose (Bloomington, IN: Indiana University Press, 1994).

Wacks, Raymond. *Personal Information: Privacy and the Law* (Oxford: Oxford University Press, 1993).

Weinberg, Jonathan. "RFID, Privacy, and Regulation" in Simson Garfinkel & Beth Rosenberg, eds. *RFID: Applications, Security, and Privacy* (Boston, MA: Addison-Wesley, 2006).

Weintraub, Jeff. "The Theory and Politics of the Private/Public Distinction" in Jeff Weintraub & Krishan Kumar, eds. *Public and Private Thought and Practice: Perspectives on a Grand Dichotomy* (Chicago: University of Chicago Press, 1997).

Westin, Alan. *Privacy and Freedom* (New York: Atheneum, 1967) at 31, 35, 36.

Whitaker, Reg. *The End of Privacy: How Total Surveillance is Becoming a Reality* (New York: New Press, 1999).

White, Michael. "Aristotle on the Infinite, Space and Time" in Georgios Anagnostopoulos, ed. *A Companion to Aristotle* (Oxford, UK: Wiley & Sons, 2009) 260.

Williams, Amanda, Eric Kabisch & Paul Dourish. "From Interaction to Participation: Configuring Space Through Embodied Interaction" in Michael Beigl, Stephen Intille, Jun Rekimoto & Hideyuk Tokuda. *Lecture Notes in Computing Science: Ubicomp 2005* (Berlin: Springer, 2005) 287.

Wittgenstein, Ludwig. *Philosophical Investigations*, 2nd ed, translated by GEM Anscombe,1968 (Oxford: Basil Blackwell, 1958).

Wittgenstein, Ludwig. *Tractatus Logico-Philosophicus*, translated by DF Pears & BF McGuinnes, 1961 (London: Routledge 1921).

Wittgenstein, Ludwig. *Zettel*, translated by GEM Anscombe & Georg H Von Wright (Oxford: Blackwell, 1967).

Young, Iris Marion. "House and Home: Feminist variations on a theme" in *Intersecting Voices: Dilemmas of gender, political philosophy, and policy* (Princeton, NJ: Princeton University Press, 1997).

Zuboff, Shoshana. *In the Age of the Smart Machine: the Future of Work and Power* (New York: Basic Books, 1988).

Zureik, Elia et al, eds. *Surveillance, Privacy and the Globalization of Personal Information* (Montreal: McGill-Queens University Press, 2010).

Secondary Material: Articles

Abowd, Gregory & Elizabeth Mynatt. "Charting Past, Present & Future Research in Ubiquitous Computing" (March 2002) 7:1 ACM Transactions on Computer-Human Interaction 29 at 32.

Agre, Philip. “Changing Places: Contexts of Awareness in Computing” (2001) 16 ACM Transactions on Computer-Human Interaction 177.

Albrechtslund, Anders. “House 2.0: Towards an Ethics for Surveillance in Intelligent Living and Working Environments” in (2007) Proceedings of CEPE 2007, International Conference of Computer Ethics: Philosophical Enquiry 7.

Albrechtslund, Anders. “The Postmodern Panopticon: Surveillance and Privacy in the Age of Ubiquitous Computing” (2005) Proceedings of CEPE 2005, International Conference of Computer Ethics: Philosophical Enquiry 17.

Ammari, Habib & Sajal Das, “Integrated Connectivity in Wireless Networks: A Two-dimensional Percolation Problem” (2008) 57:10 IEEE Transactions on Computers 1423.

Antle, Alissa, Greg Corness & Milena Dromeva. “Human-Computer Intuition: Exploring the Cognitive Basis for Intuition in Embodied Interaction” (2009) 2:3 International Journal of Arts and Technology 235.

Austin, Lisa. “Privacy and Private Law: The Dilemma of Justification” (2010) 55 McGill Law Journal 165 at 202-204.

Austin, Lisa. “Privacy and the Question of Technology” (2003) 22:2 Law & Philosophy 119.

Awan, Usman. “Wireless Intelligent Bed Sensing System” (B Eng (Hons) Thesis, Massey University, School of Engineering and Advanced Technology, 2009) [unpublished].

Bailey, Jane. “Across the Rubicon and into the Apenninies: Privacy and Common Law Police Powers after *A.M*. and *Kang-Brown*” (2009) 55 Criminal Law Quarterly 239.

Bailey, Jane. “Framed by Section 8: Constitutional Protection of Privacy in Canada” (2008) 50:3 Canadian Journal of Criminology and Criminal Justice 279.

Barnes, Trevor & Michael Curry, “Towards a contextualist approach to geographical knowledge” (1983) 8:4 Transactions of the Institute of British Geographers 467.

Bedi, Monu. “Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply” (2013) 54:1 BCL Rev 1.

Bell, Genevieve & Paul Dourish. “Yesterday’s Tomorrows: Notes on Ubiquitous Computing Dominant Vision” (2007) 11:2 Personal & Ubiquitous Computing 133.

Bellotti, Victoria & Keith Edwards, "Intelligibility and Accountability: Human Considerations in Context-Aware Systems" (2001) 16:2-4 ACM Transactions on Computer-Human Interaction 193.

Benn, Stanley. "Privacy, Freedom & Respect for Persons" (1971) 13:1 Nomos 26.

Bennett, Colin J & Priscilla M Regan, "Surveillance and Mobilities" (2003) 1:4 Surveillance & Society 449.

Beresford, Alastair R. "Location Privacy in Pervasive Computing" (2003) 2:1 IEEE Pervasive Computing 46.

Blitz, Marc Jonathon. "The Dangers of Fighting Terrorism with Techcommunitarianism: Constitutional Protections of Free Expression, Exploration and Unmonitored Activity in Urban Spaces" (2004) 32 Fordham Urban Law Journal 677.

Bloustein, Edward. "Privacy as an Aspect of Human Dignity" (1964) 39 NYU Law Review 962.

Boesen, Julie, Jennifer A Rode & Clara Mancini. "The Domestic Panopticon: Location Tracking in Families" (2010) Proceedings of Ubicomp '10, 12th ACM International Conference on Ubiquitous Computing 65.

Bohn, Jurgen et al. "Living in a World of Smart Everyday Objects – Social, Economic and Ethical Implications" (2004) 10:5 Human & Ecological Risk Assessment 763 at 771.

boyd, dana. "Facebook's Privacy Trainwreck" (2008) 14:1 Convergence: The International Journal of Research into New Media Technologies 13.

Brewer, Johanna & Paul Dourish. "Mobility, Technology and Environmental Knowing" (2008) 66:12 International Journal of Human-Computer Interaction 963.

Bruce, Harry, William P, Jones & Susan T Dumais. "Information behavior that keeps found things found" (2004) 10:1 Information Research, online: Information Research <http://informationr.net/ir/10-1/paper207.html>.

Buttimer, Anne. "Grasping the Dynamism of Lifeworld" (1976) 66:2 Annals of the American Geographers 277-292.

Calo, Ryan. "The Boundaries of Privacy Harm" (2011) 86:3 Indiana Law Journal 1131.

Clarke, Roger. "Information Technology and Dataveillance" (1988) 31:5 Communications of the ACM 498.

Coaffee, Jon. “Rings of Steel, Rings of Concrete and Rings of Confidence: Designing Out Terrorism in London” (2004) 28:1 International Journal of Urban & Regional Research 201.

Cockfield, Arthur. “Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies” (2007) 40 UBC Law Review 41.

Cohen, Julie. “A Right to Read Anonymously: A Closer Look at ‘Copyright Management’ in Cyberspace” (1996) 28 Connecticut Law Review 981.

Cohen, Julie. “DRM and Privacy” (2003) 18 Berkeley Tech Law Journal 575.

Cohen, Julie. “Examined Lives: Informational Privacy and the Subject as Object” (2000) 52 Stanford Law Review 1373.

Cohen, Julie. “Overcoming Property: Does Copyright Trump Privacy?” (2002) University of Illinois Journal of Law, Technology & Policy 375.

Cohen, Julie. “Privacy, Visibility, Transparency and Exposure” (2008) 75:1 University of Chicago Law Review.

Convoy, Amy. “Protecting Your Personality Rights in Canada: A Matter of Property or Privacy” (2012) 1:1 Western Journal of Legal Studies 3.

Crabtree, Andy & Tom Rodden. “Hybrid Ecologies: Understanding Co-operative Interaction in Emerging Physical-Digital Environments” (2008) 12:7 Personal & Ubiquitous Computing 481.

Craven, JB. “Personhood: The Right to Be Let Alone” (1976) Duke Law Journal 699.

Cresswell, Tim. “The Production of Mobilities” 43 New Formations 11-25.

Crowley, James et al. “Perceptual Components for Context Aware Computing” (2002) 2498 Ubicomp 2002: Ubiquitous Computing, Lecture Notes in Computer Science 117-134.

Cuff, Dana. “Immanent Domain: Pervasive Computing and the Public Realm” (2002) Journal of Architectural Education 43.

Davenport, Mae & Dorothy Anderson. “Getting from sense of place to place-based management: An interpretive investigation of place meanings and perceptions of landscape change” (2005) 18:7 Society & Natural Resources 625-641.

de Ipina, Diego Lopez et al. “TRIP: A Low Cost Vision-Based Location System for Ubiquitous Computing” (2002) 6:3 Journal of Personal and Ubiquitous Computing 206.

de Souza e Silva, Adriana & Jordon Firth. “Locational Privacy” (2010) 3:4 Communication, Culture and Critique 503.

de Souza e Silva, Adriana. “From Cyber to Hybrid: Mobile Technologies as Interfaces of Hybrid Spaces” (2006) 9:3 Space and Culture 261.

van den Hoven, Jeroen & Pieter E Vermaas. “Nano-Technology and Privacy: On Continuous Surveillance Outside the Panopticon” (2007) 32:3 Journal of Medicine & Philosophy 283 at 292.

Dey, Anind, Peter Ljungstrand & Albrecht Schmidt. “Distributed & Disappearing User Interfaces in Ubiquitous Computing” (2001) CHI 487.

Dey, Anind. “Understanding and Using Context” (2001) 5:1 Personal Ubiquitous Computing 4-7.

Doty, Nick & Erik Wilde. “Geolocation Privacy and Application Platforms” (2010) Proceedings of 3rd ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS 65.

Edney, Julian. “Human Territoriality” (1974) 81 Psychological Bulletin 959.

Edwards, W Keith & Rebecca E Grinter, “At Home with Ubiquitous Computing: Seven Challenges” (2001) Proceedings of 3rd International Conference on Ubiquitous Computing 256.

Encarnação**,** José. “Ambient Intelligence: The New Paradigm for Computer Science and for Information Technology” (2008) 50:1 IT–Information Technology 5.

Epstein, Richard. “The Legal Regulation of Genetic Discrimination: Old Responses to New Technology” (1994) 74:1 Boston University Law Review 13.

Escobar, Arturo. “Culture Sits in Places” (2001) 20:2 Political Geography 139-174.

Fairclough, Stephen H. “Fundamentals of Physiological Computing” (2009) 21:1-2 Interacting with Computers 133.

Ferneley, Elaine & Ben Light, “Unpacking User Relations in an Emerging Ubiquitous Computing Environment: Introducing the Bystander” (2008) 23:3 Journal of Information Technology 163.

Ferscha, Alois. “20 Years Past Weiser: What’s Next?” (2012) 11:1 IEEE Pervasive Computing 52.

Fishkin, Kenneth “Embodied User Interfaces: Towards Invisible User Interfaces” (1998) Engineering for Human Computer Interaction 4.

Fishkin, Kenneth. “A Taxonomy for and Analysis of Tangible Interfaces” (2004) 8:5 Journal of Personal and Ubiquitous Computing 347.

Fried, Charles. “Privacy” (1968) 77 Yale Law Journal 475.

Friedewald, Michael et al. “Perspectives of Ambient Intelligence in the Home Environment” (2005) 22:3 Telematics and Informatics 221.

Froomkin, Michael. “The Death of Privacy” (2000) 52 Stanford Law Review 1461.

Fuji, A. “Trends and Issues in Research on Context Awareness Technologies for a Ubiquitous Network Society” (November 2008) NISTP Science and Technology Trends 092.

Galloway, Anne. “Imitations of Everyday Life: Ubiquitous Computing and the City” (2004) 18:2-3 Cultural Studies 384.

Gavison, Ruth. “Feminism and the Public-Private Distinction” (1992) 45:1 Stanford Law Review 1.

Gavison, Ruth. “Privacy and the Limits of Law” (1980) 89 Yale Law Journal 412.

Gavison, Ruth. “Too Early for a Requiem” (1992) 43 South California Law Review 437.

Gershenfeld, Neil, Raffi Krikorian & Dany Cohen. “The Internet of Things” *Scientific American* 291:4 (2004) 76.

Gibbs, Wayt “As We May Live” *Scientific American* (November 2000) 36.

Gold, Rich. “This is not a Pipe” (1993) 36 Communications of the ACM 72.

Graham, Stephen & David Wood. “Digitalizing Surveillance” (2003) 23:2 Critical Social Policy 227.

Green, Nicola. “On The Move: Technology, Mobility and the Mediation of Social Time and Space” (2002) 65 Law & Contemporary Problems 125 at 152.

Greenfield, Adam. “Everyware: Some Social and Ethical Implications of Ubiquitous Computing” (Keynote address, delivered at Pervasive 2007, the 5th International Conference on Pervasive Computing, Toronto, Canada, 14 May 2007).

Gustafson, Per. “Meanings of Place: Everyday Experience and Theoretical Conceptualizations” (2001) 21:1 Journal of Environmental Psychology 5-16.

Haggerty, Kevin D & Richard V Ericson, “The Surveillant Assemblage” (2000) 51:4 British Journal of Sociology 605.

Hannam, Kevin et al. “Mobilities, Immobilities and Moorings” (2006) 1:1 Mobilities 1-22.

Hay, Robert. “Sense of Place in Development Context” (1998) 18:1 Journal of Environmental Psychology 5-29.

Henkin, Louis. “Privacy & Autonomy” (1974) 74 Columbia Law Review 1410.

Hornecker, Eva & Jacob Buur. “Getting a Grip on Tangible Interaction: A Framework on Physical Space and Social Interaction” (2006) Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM 437.

Hornecker, Eva et al. “TEI Goes On: Tangible and Embedded Interaction” (2008) 7:2 IEEE Pervasive Computing 91.

Horowitz, Morton. “The History of the Public-Private Distinction” (1982) 130(6) University of Pennsylvania Law Review 1423.

Huhtamo, Erkki. “Armchair Traveller and the Virtual Voyager” (1995) 6:2-3 Mediamatic 13.

Hunter, Dan. “Cyberspace as Place and the Tragedy of the Digital Anti-commons” (2003) 91:2 California Law Review 439.

Ishii, Hiroshi & Brygg Ullmer. “Tangible Bits: Towards Seamless Interfaces Between People, Bits and Atoms” (1997) Proceedings of CHI97, ACM 234.

Ishii, Hiroshi. “The Tangible User Interface and Its Evolution” (2008) 51:6 Communications of the ACM 32.

Johnston, David R & David G Post. “Law and Borders: The Rise of Cyberspace” (1996) 48 Stanford Law Review 1367.

Jorgensen, Bradley & Richard Stedman. “Sense of Place as an Attitude” (2001) 21 Journal of Environmental Psychology 233-248.

Kabisch, Eric. “Datascape: A Synthesis of Digital and Embodied Worlds” (2008) 11:3 Space and Culture 222.

Kakihara, Maso & Carsten Sorenson. “Expanding the Mobility Concept” (2001) 22:3 Communications of the ACM 33.

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

Kaytal, Sonia. “The New Surveillance” (2004) 54 Case Western Law Review 297.

Kerr, Ian & Jena McGill. “Emanations, Snoop Dogs and Reasonable Expectations of Privacy” (2007) 52:3 Criminal Law Quarterly 392.

Kerr, Ian, Cynthia Aoki & Max Binnie. “Tessling on My Brain: The Future of Lie Detection and Brain Privacy in the Criminal Justice System” (2008) 50:8 Canadian Journal of Criminology and Criminal Justice 367.

Kerr, Ian. “Bots, Babes and the Californication of Commerce” (2004) 1 Ottawa Law and Technology Journal 285-325.

Klemmer, Scott. “Integrating Physical and Digital Interactions” *Computer* (2005) 111.

Konvitz, Milton. “Privacy and the Law: A Philosophical Prelude” (1966) 31 Law & Contemporary Problems 272.

Koops, Bert-Jaap & Merel M Prinsen. “Houses of Glass, Transparent Bodies: How New Technologies Affect Inviolability of the Home and Bodily Integrity in the Dutch Constitution” (2007) 16:3 Information & Communication Technology Law 177 at 184.

Koskela, Hille. “CamEra: The Contemporary Urban Panopticon” (2003) 1:3 Surveillance & Society 292-313.

Koskela, Hille. “The Gaze Without Eyes: Video Surveillance and the Changing Nature of Urban Space” (2000) 24 Progress in Human Geography 243

Koskela, Hille. “Webcams, TV Shows and Mobile Phones: Empowering Exhibitionism” (2004) 2:2-3 Surveillance & Society 199.

Lahlou, S et al. “Privacy and Trust Issues with Invisible Computers” (2005) 48:3 Communications of the ACM 59.

Lemley, Mark. “Place and Cyberspace” (2003) 91 California Law Review 521.

Lemos, Andre. "Post-Mass Media Functions, Locative Media and Informational Territories: New Ways of Thinking About Territory, Place and Mobility in Contemporary Society" (2010) 13:4 Space and Culture 403-420.

Lyon, David. "Surveillance Studies: Understanding Visibility, Mobility and the Phenetic Fix" (2002) 1:1 Surveillance & Society 1.

Lyytinen, Kalle & Youngjin Yoo. "Issues and Challenges in Ubiquitous Computing" (2002) 45 Communications of the ACM 63.

MacKinnon, William. "Tessling, Brown and A.M.: Towards a Principled Approach in Section 8" (2007) 45 Alberta Law Review 79.

Manovich, Lev. "The Poetics of Augmented Space" (2002) 5(2) Visual Communication 219.

Manzo, Lynn. "Beyond House and Haven: Toward a Revision of Emotional Relationships with Places" (2003) 23:1 Journal of Environmental Psychology 47-61.

Manzo, Lynn. "For Better or Worse: Exploring Multiple Dimensions of Place Meaning" (2005) 25:1 Journal of Environmental Psychology 67-86.

Marx, Gary. "An Ethics for the New Surveillance" (1998) 14:3 The Information Society 171.

Marx, Gary. "Murky Conceptual Waters: The Public and the Private" (2001) 3:3 Ethics and Information Technology 157.

Marx, Gary. "What's New About the "New Surveillance"? Classifying for Change and Continuity" (2002) 1:1 Surveillance & Society 9-29.

Matheson, David. "Deeply Personal Information and the Reasonable Expectation of Privacy in *Tessling*" (2008) 50:3 Canadian Journal of Criminology and Criminal Justice 349.

McCarthy, John, Peter Wright, Jane Wallace & Andy Deardon. "The Experience of Enchantment in Human-Computer Interaction" (2006) 10:6 Journal of Personal and Ubiquitous Computing 369.

McCullough, Malcolm. "On the Urbanism of Locative Media" (2006) 18:2 Places 26.

McGowen, David. "The Trespass Trouble and the Metaphor Muddle" (2005) 1 Journal of Law, Economics & Policy 109.

Mehta, Michael D. “On Nano-Panopticism: A Sociological Perspective” (2002) 54:10 Canadian Chemical News 31.

Merriman, Peter et al. “Landscape, Mobility and Practice” (2008) 9 Social and Cultural Geography 191-212.

Michael, Katrina & MG Michael. “Nanotechnology: The Growing Impact of Shrinking Computers” (2006) 1 IEEE Pervasive Computing 1.

Michael, MG & Katina Michael. “Microchipping People: The Rise of the Electrophorus” (2005) 49:3 Quadrant 22.

Michael, MG & Katina Michael. “Towards a State of Uberveillance” (2010) 19:2 IEEE Technology and Society Magazine 9.

Michael, MG & Katina Michael. “Uberveillance: Microchipping People and the Assault on Privacy” (2009) 53:3 Quadrant 85.

Mironenko, Olga. “Body Scanners Versus Privacy Versus Data Protection” (2011) 27 Computer Law & Security Review 232-244.

Mitra, Amanda & Rae Lynn Schwartz. “From Cyberspace to Cybernetic Space: Rethinking the Relationship Between Real and Virtual Spaces” (2001) 1 Journal of Computer-Mediated Communication 7.

Monahan, Torin. “War Rooms of the Street: Surveillance Practices in Transportation Control Centres” (2007) 10 The Communication Review 367.

Moreham, Elizabeth. “Privacy in the Common Law: A Doctrinal and Theoretical Analysis” (2005) 121 Law Quarterly Review 628.

Murphy, Richard S. “Property Rights in Personal Information: An Economic Defense of Property” (1996) 84 Georgetown Law Journal 2381.

Nagel, Thomas. “Concealment and Exposure” (1998) 27 Philosophy & Public Affairs 3.

Nath, Badi, Frank Reynolds & Roy Want. “RFID Technology and Applications” (2006) 5:1 IEEE Pervasive Computing 22.

Nissenbaum, Helen et al. “Privacy and Contextual Integrity: Framework and Applications” (May 2006) Proceedings of the 27th IEEE Symposium on Security & Privacy 184.

Nissenbaum, Helen. “Privacy as Contextual Integrity” (2004) 79:1 Washington Law Rev 119 at 137.

Nissenbaum, Helen. “Protecting Privacy in an Information Age: the Problem with Privacy in Public” (1998) 17 Law & Philosophy 559 at 579.

Ooi, Chin, Kian Lee Tam & Anthony Tung. “Sense the Physical, Walk Through the Virtual, Manage the Co (existing) Spaces: A Database Perspective” (2009) 38:3 SIGMOD Record 5.

Palen, Leysia & Paul Dourish. “Unpacking Privacy in a Networked World” (2003) Proceedings of CHI’03, SIGCHI Conference on Human Factors in Computing Systems 129.

Paton-Simpson, Elizabeth. “Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places” (2000) 50 University of Toronto Law Journal 305.

Pecora, Vincent P. “The Culture of Surveillance” (2002) 25:3 Qualitative Sociology 345.

Penny, Steven. “Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach” (2007) 97 Journal of Criminal Law & Criminology 477.

Perusco, Laura & Katina Michael. “Control, Trust, Privacy, and Security: Evaluating Location-Based Services” (2007) 26:1 IEEE Technology and Society 4.

Picard, Rosalind W, Elias Vyzas & Jennifer Healey, “Toward Machine Emotional Intelligence: Analysis of Affective Physiological State” (2001) 23:10 IEEE Transaction on Pattern Analysis and Machine Intelligence 1175.

Post, Robert. “The Social Foundations of Privacy: Community and Self in the Common Law Tort” (1989) 77 California Law Review 957.

Rachels, James. “Why Privacy is Important” (1975) 4 Philosophy & Public Affairs 323.

Radin, Magaret Jane. “Property and Personhood” (1982) 34 Stanford Law Review 957.

Rehman, Kasmin, Frank Stajano & George Coulouris. “Interfacing with the Invisible Computer” (2002) CHI 213.

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

Reiman, Jeffrey. “Privacy, Intimacy & Personhood” (1976) 6 Philosophy & Public Affairs 26.

Reynolds, Carson & Rosalind Picard. “Affective Sensors, Privacy and Ethical Contracts” (2004) Proceeding of CHI ’04 Extended Abstracts on Human Factors in Computing Systems 1103.

Richards, Neil. “Intellectual Privacy” (2008) 87 Texas Law Review 387.

Richards, Neil. “The Dangers of Surveillance” (2012) Harvard Law Review, online cite from FN.

Rowe, David. “Euclidean Geometry and Physical Space” (2006) 28:2 The Mathematical Intelligencer 51-59, 53.

Rubenfeld, Jeb. “The Right to Privacy” (1989) 102 Harvard Law Review 737.

Satyanarayanan, Mahader. “Pervasive Computing: Visions and Challenges” (2001) 8:4 IEEE Personal Communications 15.

Scassa, Teresa. “Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy” (2010) 7:2 Canadian Journal of Law and Technology 193 at 195.

Schilit, Bill & Marvin Theimer. “Disseminating Active Map Information to Mobile Hosts” (1994) 8:5 IEEE Network 22.

Schmidt, Albrecht et al. “Interacting with 21st Century Computers” (2012) 11:1 IEEE Pervasive Computing 22.

Schmidt, Albrecht et al. “There is More to Context than Location” (1999) 23 Computers & Graphics 893.

Sewell, Graham & James Barker, “Neither Good, nor Bad, but Dangerous: Surveillance as an Ethical Paradox” (2001) 3:3 Journal of Ethics and Information 181.

Sheller, Mimi & John Urry. “The New Mobilities Paradigm” (2006) 38:2 Environment & Planning A 207 at 221.

Sheller, Mimi and John Urry. “Mobile Transformations of ‘Public’ and the ‘Private’ Life” (2003) 20(3) Theory, Culture, and Society 107.

Slane, Andrea. “From Scanning to Sexting: The Scope of Protection of Dignity-Based Privacy in Canadian Child Pornography Law” (2010) 48 Osgood Hall LJ 543.

Solove, Daniel. “Privacy and Power: Computer Databases and Metaphors for Information Privacy” (2001) 53 Stanford Law Review 1393-1462.

Spiekerman, Sarah & Frank Pallas. "Technology Paternalism: Wider Implications of Ubiquitous Computing" (2006) 4:1 International Journal Ethics of Science & Technology Assessment 1615.

Stedman, Richard. "Is it really a social construction?: The contribution of the physical environment to sense of place" (2003) 16:8 Society & Natural Resources 671-685.

Steeves, Valerie. "If the Supreme Court Were on Facebook: Evaluating the Reasonable Expectation of Privacy Test from a Social Perspective" (2008) 50(3) Canadian Journal of Criminology and Criminal Justice 331.

Swift, Adam. "Locating 'Agency' Within Ubiquitous Computing Systems" (2007) 8 International Review of Information Ethics 36.

Taslitz, Andrew E. "The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions" (2002) 65:2 Law & Contemporary Problems 125

Thomson, Judith Jarvis. "The Right to Privacy" (1974) Philosophy & Public Affairs 4.

Trudeau, Pierre Elliot, in Geoffrey Stevens. "Bill Overhauls Criminal Code" (Ottawa, Canada, December 21, 1967) *The Globe and Mail* (22 December 1967) 1.

Tuan, Yi-Fu. "A View of Geography" (1991) 81:1 Geographical Review 99 at 101

Tuan, Yi-Fu. "Space and Place: Humanistic Perspective" (1974) 6 Progress in Human Geography 211-252.

Turing, Alan. "Computing Machinery and Intelligence" (1950) 59 Mind 433 at 433.

van den Hoven, Elise et al. "Design Research and Tangible Interaction" (2007) Proceedings of the International Conference on Tangible and Embedded Interaction, ACM 109.

Wacks, Robert. "The Poverty of Privacy" (1980) 96 Law Quarterly Review 73 at 75-77.

Wang, Patrick SP & Svetlana N Yanushkevich, "Biometric Technologies and Applications" (2007) Proceedings of 25th IASTED International Multi-Conference: Artificial Intelligence and Applications 226.

Want, Roy et al. "The Active Badge Location System" (1992) 10:1 ACM Transactions on Information Systems 92.

Want, Roy, Trevor Pering, Gaetano Borriello & Keith Farkas. "Disappearing Hardware" (2002) 1:1 IEEE Pervasive Computing 36 at 42.

Warren, Samuel D & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harvard Law Review 193.

Weiser, Mark "The Technologist's Responsibilities and Social Change" *Computer-Mediated Communication Magazine* 2:4 (April 1995) 17.

Weiser, Mark, John Seely-Brown & Rich Gold. "The Origins of Ubiquitous Computing Research at PARC in the late 1980's" (1999) 38:4 IBM Systems Journal 693.

Weiser, Mark. "Creating the Invisible Interface" (1994) Proceedings of the 7th Annual Symposium on User Interface Software and Technology 1.

Weiser, Mark. "Some Computer Issues for Ubiquitous Computing" (July 1993) 36:7 Communications of the ACM 75.

Weiser, Mark. "The Computer for the 21st Century" *Scientific American* 265:3 (1991) 66.

Weiser, Mark. "The Technologist's Responsibilities and Social Change" *Computer-Mediated Communication Magazine* 2:4 (April 1995) 17.

Weiser, Mark. "The World is not a Desktop" (1994) 1:1 Interactions 7.

Wellner, Pierre. Wendy MacKay & Rich Gold "Back to the Real World" (July 1993) 3:7 Communications of the Association of Computing Machinery (ACM) 24.

Werbach, Kevin D. "Sensors and Sensibility" (2007) 28:1 Cardozo Law Review 2321 at 2321.

Westin, Alan. "Social and Political Dimensions of Privacy" 59:2 2003 Journal of Social Issues 431-453.

Wood, David M. "The 'Surveillance Society': Questions of History, Place and Culture" (2009) 6:2 European Journal of Criminology 179.

Zick, Timothy. "The First Amendment and Networked Public Places" (2007) 59:1 Florida Law Review 1.

Zimmer, Michael. "Book Review of: *Theorizing Surveillance: The Panopticon and Beyond by David Lyon, ed.*" (2008) 5:2 Surveillance & Society 203 at 203.

Zimmer, Michael. "Privacy on Planet Google" (2008) 3 Journal of Business & Technology 109.

Zimmer, Michael. "Surveillance, Privacy and the Ethics of Vehicle Safety" (2005) 7 Ethics & Information 201.

Secondary Material: Online & Media Resources

"A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace" (1996) 28 Conn L Rev 98, online: Georgetown University <http://www.law.georgetown.edu/faculty/jec/read_anonymously.pdf>.

"Exposure" online: Word Reference <http://www.wordreference.com/definition/exposure>.

"Finishing the Job" *The Economist*, A Special Report on Telecoms in Emerging Markets (26 September 2009) 13, online: The Economist <http://www.economist.com/node/14483856>.

"Judge Allows GPS Evidence in Peterson Case" *CNN.com* (17 February, 2004), online: CNN.com <http://www.cnn.com/2004/LAW/02/17/peterson.trial/index.html>.

"Schott's Vocab: Uberveillance" (4 February 2009), online: New York Times <http://schott.blogs.nytimes.com/2009/02/04/uberveillance/>.

"Smarter on the way" 19th World Congress on Intelligent Transport Systems (25-26 October 2012), online: 19th ITS World Congress <http://2012.itsworldcongress.com/content>.

"Things That Think Consortium" online: MIT Media Lab <http://ttt.media.mit.edu/>.

"Wow! The foursquare community has over 10,000,000 members!" (June 20, 2011), online: Foursquare Blog <http://blog.foursquare.com/2011/06/20/holysmokes10millionpeople/>.

Article 29 Data Protection Working Party. "Working document on data protection issues related to RFID technology" (19 January 2005), online: European Commission Article 29 Working Party <http://ec.europa.eu/justice/data-protection/article-29/>.

Ashton, Kevin. "That 'Internet of Things' Thing" (June 2009) RFID Journal, online: Radio Frequency Technology News & Features <http://www.rfidjournal.com/article/view/4986>.

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

Barlow, John Perry. "A Declaration of the Independence of Cyberspace," online: Electronic Frontier Foundation <http://projects.eff.org/~barlow/Declaration-Final.html>.

Beresford, Alastair R. "Location Privacy in Ubiquitous Computing" Technical Report UCAM-CL-TR-612 (2005), online: University of Cambridge Computer Laboratory <http://www.cl.cam.ac.uk/techreports/>.

Bleecker, Julian. "Why Things Matter", online: Scribd <http://www.scribd.com/doc/14748019/Why-Things-Matter>.

Bush, Vannevar. "As We May Think,"*Atlantic Monthly* (July 1945) 101, online: The Atlantic <http://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/303881/>.

Butler, Don. "The Surveillance Society, Part VI: Everyone's Watching" *Ottawa Citizen* (9 February 2009), online: Ottawa Citizen <http://www.ottawacitizen.com/Part+Everyone+watching/1253557/story.html>.

Carnegie Mellon University, "Project Aura," online: Aura <http://www.etc.cmu.edu/projects/aura>.

Casey, Edward. "Between Geography and Philosophy: What Does it Mean to be in the Place-World" (2001) 91:4 Annals of the American Geographers 683-693.

Cavoukian, Ann. "Privacy By Design," online: Information and Privacy Commissioner of Ontario <http://www.privacybydesign.ca>.

Chirgwin, Richard. "Why we should be afraid of Google Street View," *APC Magazine* (11 August 2008), online: APCMag.com <http://apcmag.com/why_we_should_be_afraid_of_google_streetview.htm>.

Corning. "A Day Made of Glass," online: YouTube <http://www.youtube.com/watch?v=6Cf7IL_eZ38>

Council on the Internet of Things think-tank, online: The Internet of Things <http://www.theinternetofthings.eu/>.

Dennis, Kingsley L. "New Instruments of Surveillance and Social Control", Global Research (2008), online: Global Research <http://www.globalresearch.ca/new-

instruments-of-surveillance-and-social-control-wireless-technologies-which-target-the-neuronal-functioning-of-the-brain/8263>.

Department of Electrical Engineering and Computer Sciences, University of California Berkeley, "Mark Weiser dies at 46" (1999 obituary), online: UC Berkeley Electrical Engineering and Computer Sciences <http://www.cs.berkeley.edu/Weiser/bio.shtml>.

Dey, Anind & Gregory Abowd. "Towards a Better Understanding of Context and Context-Awareness" (2001) GVU Technical Report GIT-GVU 99-22, online: Georgia Tech Library SMARTech <http://smartech.gatech.edu/handle/1853/3389>.

Forberg, Sigrid. "Taking to the skies: New tool facilitates investigations" (2012) 74:1 Gazette, online: Royal Canadian Mounted Police <http://www.rcmp-grc.gc.ca/gazette/vol74n1/trends-dernierestendances-eng.htm>.

Foursquare. online: <http://foursquare.com>.

Gale International, "SongdoIBD," online: Songdo <http://songdo.com>.

Get Smart, television, NBC/CBS (1965-70), "Get Smart title sequence", online: YouTube < http://www.youtube.com/watch?v=ElqZms_SUjg>.

Gibson, William. "The Road to Oceania" *New York Times* (25 June 2003), online: New York Times Opinion <http://www.nytimes.com/2003/06/25/opinion/the-road-to-oceania.html>.

Google. "Our History in Depth," online: Google <http://www.google.ca/about/company/history/#2007>.

Google. "Project Glass," online: <http://www.youtube.com/watch?v=9c6W4CCU9M4>.

Greenfield, Adam. "All Watched Over By Machines of Loving Grace: Some Ethical Guidelines for User Experience in Ubiquitous Computing Settings" (1 December 2004), online: Boxes and Arrows <http://boxesandarrows.com/all-watched-over-by-machines-of-loving-grace-some-ethical-guidelines-for-user-experience-in-ubiquitous-computing-settings-1/>.

Hewlett-Packard. "Cooltown," online: Hewlett-Packard <http://cooltown.com>

Honan, Mathew. "I Am Here" *Wired* (February 2009), online: Wired <www.wired.com/gadgets/wireless/magazine/17-02/lp_guineapig>.

Hubbard, Ben. "Police Turn to Secret Weapon: GPS, Device," *The Washington Post (*13 August 2008), online: The Washington Post <http://www.washingtonpost.com/wp-dyn/content/article/2008/08/12/AR2008081203275.html >.

Ikea. "Mother of All Kitchens" (12 August 2010), online: Ikea News Room <http://www.ikea.com/gb/en/about_ikea/newsitem/UK_kitchen_news_release >.

Ip, Rodney, Katina Michael & M G Michael. "Toward Chipification: The Multifunctional Body," online: University of Wollongong, Faculty of Informatics <http://ro.uow.edu.au/infopapers/372/>.

Ip, Rodney, Katrina Michael & M G Michael. "The Social Implications of Human-centric Chip Implants: Thy Chipdom Come, Thy Will Be Done," online: University of Wollongong, Faculty of Informatics <http://ro.uow.edu.au/infopapers/601/>.

ITU Report, "Mobile Technologies: Towards a Converged World" (2004), online: International Telecommunication Union <http://itu.int/osg/spu/ni/futuremobile/broadbandmobile.pdf>.

ITU Telecommunication Standardization Sector, *ITU-T Workshop Report on Networked RFID: Systems and Services, Geneva, 2006* (Geneva, ITU-T, 2006), online: International Telecommunication Union <http://www.itu.int/ITU-T/worksem/rfid/>.

Justice La Forest, Gérard**.** "Opinion – Video Surveillance" (5 April 2002), online: Office of the Privacy Commissioner of Canada Archived News <https://www.priv.gc.ca/media/nr-c/opinion_020410_e.asp>.

Kingsley, Sam. "Cellspace: The Prototype for a New Society," online: SamKinsley.com <*www.samkinsley.com/archives/000019.html>.*

Kostakos, Vassilis & Eamonn O'Neill. "A Space-oriented Approach to Designing Pervasive Systems," online: University of Bath, Department of Computer Science <http://www.cs.bath.ac.uk/pervasive/publications/ukubinet05.pdf>.

Lorraine, Veronica. "Google Cheat View," *The Sun* (31 March 2009), online: The Sun <http://www.thesun.co.uk/sol/homepage/news/article2350771.ece>.

Massachusetts Institute of Technology, "Project Oxygen," online: MIT Oxygen Project <http://oxygen.lcs.mit.edu/>.

Massey, Doreen. "A Global Sense of Place", online: <http://www.aughty.org/pdf/global_sense_place.pdf>.

Mattern, Friedemann. “Wireless Future: Ubiquitous Computing” in Proceedings of the Wireless Congress (Munich, 2009), online: ETH Zurich, Distributed Systems Group <www.vs.inf.ethz.ch/publ/papers/mattern2004_electronica.pdf>.

Microsoft, “Future Vision @ 2020,” online: YouTube <http://www.youtube.com/watch?v=55p3vNCF4JQ>.

Moran, Thomas & Paul Dourish. “Introduction to this Special Issue on Context-Aware Computing”(2001) 16:2-3 Human Computer Interaction 87, online: Dourish.com <http://www.dourish.com/publications/2001/hci-cxt-aware-intro.pdf>.

New York Police Department. “Press Release: Midtown Manhattan Security Initiative,” online: NYPD <http://www.nyc.gov/html/nypd/html/pr/pr_2010_midtown_security_initiative.shtml>.

Nguyen, David H & Elizabeth D Mynatt, “Privacy Mirrors: Understanding and Shaping Socio-technical Ubiquitous Computing Systems” (2002) GVU Technical Report GIT-GVU 01-16, online: Georgia Tech Library <http://smartech.gatech.edu/bitstream/handle/1853/3268/02-16.pdf>.

OECD Directorate for Science, Technology and Industry. “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” (1980), online: OECD <http://www.oecd.org/sti/>.

Office of the Privacy Commissioner of Canada, Privacy & Aviation Report (2011), online: <http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_catsa_2011_e.pdf>.

Office of the Privacy Commissioner of Canada. “News Release: Google contravened Canadian privacy law, investigation finds” (19 October 2010), online: Office of the Privacy Commissioner of Canada Archived News <http://www.priv.gc.ca/media/nr-c/2010/nr-c_101019_e.asp>.

Office of the Privacy Commissioner of Canada. “RFID Technology” (23 February 2006), online: Office of the Privacy Commissioner of Canada Fact Sheets <http://www.priv.gc.ca/resource/fs-fi/02_05_d_28_e.asp>.

Opening keynote address, UBICOMP 2006, online: <http://www.luci.ics.edu/blog/archives/2006/09/ubicomp_2006_br_1.html

Philips, “Vision of the Future,” online: YouTube <http://www.youtube.com/watch?v=hvGb-o2Y_XO>.

Quinn, Jennifer. "Police drones sparks debate over personal privacy," *The Star* (5 February 2013), online: thestar.com <http://www.thestar.com>.

Rheingold, Howard. "PARC is Back," *Wired* (February, 1994), online: Wired <http://www.wired.com/wired/archive/2.02/parc_pr.html>.

Rogers. "Smart Home Monitoring," online: Rogers Home Monitoring <http://www.rogers.com>.

Rolling Stone interview with William Gibson, online: Rolling Stone <http://www.rollingstone.com/politics/story/17227831/william_gibson_the_rolling_stone_40th_anniversary_interview>.

Samsung. "Future Life and Style," online: YouTube <http://www.youtube.com/watch?v=1nKFW-lDNK8>.

Schmidt, Charles W. "The Networked Physical World," online: RAND Corporation <http://smapp.rand.org/ise/ourfuture/Internet/sec4_networked.html>.

Stadler, Felix. "The Space of Flows: Notes on the Emergence, Characteristics and Possible Impact on Physical Space," online: Notes and Nodes <http://felix.openflows.com/html/space_of_flows.html>.

Sterling, Bruce. "Spimes and The Future of Artifacts" (Keynote address, LIFT Conference, February 3, 2006), online: YouTube <http://www.youtube.com/watch?v=E2Fb7ezbVtY&feature=gv>.

Sterling, Bruce. "The Future, The Internet and the World Wide Web" (Keynote address, O'Reilly Media Emerging Technology Conference, March 2006), online: ITC Conversations <http://itc.conversationsnetwork.org/shows/detail717.html>.

Sterling, Bruce. "The Internet of Things: What is Spime and Why is it Useful" (Keynote address, Google TechTalks, April 2007), online: YouTube <http://www.youtube.com/watch?v=avCLyNRbw3Q>.

Superman, film, directed by Richard Donner (Burbank, CA: Warner Bros Entertainment Inc, 1978).

The Birds, film, directed by Alfred Hitchcock (Los Angeles, CA: Universal Pictures, 1963), "Trapped in Phone Booth clip", online: movieclips.com <http://movieclips.com/Jtys-the-birds-movie-trapped-in-a-phone-booth/>.

The Walt Disney Family Museum <www.waltdisney.org>.

Transport Canada <http://www.tc.gc.ca/eng/innovation/its-menu.htm>.

Tsibidis, George, Theodoros N Arvanitis & Chris Baber, "The What, Who, Where, When, Why and How of Context-Awareness" (Paper delivered at the Human Computer Interaction Conference, The Hague, Netherlands, April 2000), online: Georgia Tech Library SMARTech <http://smartech.gatech.edu/jspui/bitstream/1853/3464/23/00-18x.pdf>.

University of California Berkeley, "The Endeavour Expedition: Charting the Fluid Information Utility" online: Endeavor Project <http://endeavour.cs.berkeley.edu>.

"Convergence of Mobile Devices in the Physical World", video, online: YouTube <http://www.youtube.com/watch?v=6cnFwxTI4eQ>.

Warwick, Kevin. "Identity and Privacy Issues Raised by Biomedical Implants" (2002) 67 IPTS Report 29 and "Wiring in Humans" (Paper delivered at the Conference on 'Safeguards in a World of Ambient Intelligence,' Brussels, 21-22 March 2006), online: European Commission Joint Research Centre, Information Society Unit <http://is.jrc.ec.europa.eu/pages/TFS/documents/Deliverable5-ReportonConference.pdf>.

Weeks, Carly. "The Smart Phone That Knows What you Are Thinking" *The Globe and Mail* (January 2012), online: The Globe and Mail <http://www.theglobeandmail.com/technology/the-smart-phone-that-knows-what-you-want/article542362/.>

Weiser, Mark & John Seely-Brown. "Designing Calm Technology" (1996) 1 PowerGrid Journal 1, online: CiteSeerx <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.123.8091>.

Weiser, Mark. "Open House," *ITP Review 2.0*, the web magazine of the Interactive Telecommunications Program of New York University (March 1996), online: Princeton University, Computer Science Department <http://www.cs.princeton.edu/courses/archive/spring99/cs598c/papers/wholehouse.doc>.

Weiser, Mark. "User Interface, Systems, and Technologies" (ACM keynote address, November, 1994), slides online: <http://www.ubiq.com/hypertext/weiser/UbiHome.html>.

Wikipedia, sub verbo "Dasein", literal translation: "there" [Da] plus "being" [Sein], online: Wikipedia <http://en.wikipedia.org/wiki/Dasein>.

Wired Magazine: Kevin Kelly, "Predicting the Next 5000 Days of the Web" (2007), online: YouTube <http://www.youtube.com/watch?v=yDYCf4ONh5M>.

Zirin, Dave. "Drones, missiles and gunships: Welcome to the 2012 London Olympics," *The Star* (21 May 2012), online: thestar.com <www.thestar.com>.