Geo-Immersive Surveillance &
Canadian Privacy Law

By

Stuart Andrew Hargreaves

A thesis submitted in conformity with the requirements for the degree of Doctor of Juridical Science.

Faculty of Law

University of Toronto

© Copyright by Stuart Hargreaves (2013)
Geo-Immersive Surveillance & Canadian Privacy Law

Stuart Andrew Hargreaves

Doctor of Juridical Science
Faculty of Law, University of Toronto
2013

Abstract

Geo-immersive technologies digitally map public space for the purposes of creating online maps that can be explored by anyone with an Internet connection. This thesis considers the implications of their growth and argues that if deployed on a wide enough scale they would pose a threat to the autonomy of Canadians. I therefore consider legal means of regulating their growth and operation, whilst still seeking to preserve them as an innovative tool. I first consider the possibility of bringing ‘invasion of privacy’ actions against geo-immersive providers, but my analysis suggests that the jurisprudence relies on a ‘reasonable expectation of privacy’ approach that makes it virtually impossible for claims to privacy ‘in public’ to succeed. I conclude that this can be traced to an underlying philosophy that ties privacy rights to an idea of autonomy based on shielding the individual from the collective. I argue instead considering autonomy as ‘relational’ can inform a dialectical approach to privacy that seeks to protect the ability of the individual to control their exposure in a way that can better account for privacy claims made in public. I suggest that while it is still challenging to craft a private law remedy based on such ideas, Canada’s data protection legislation may be a more suitable vehicle. I criticize the Canadian Privacy Commissioner’s current approach to geo-immersive technologies as inadequate, however, and instead propose an enhanced application of the substantive requirements under Schedule 1 of PIPEDA that is consistent with a relational approach to privacy. I suggest this would serve to adequately curtail the growth of geo-immersive technologies while preserving them as an innovative tool. I conclude that despite criticisms that ‘privacy’ is an inadequate remedy for the harms of surveillance, in certain commercial contexts the fair information principles can, if implemented robustly, serve to regulate the collection of personal information ‘at source’ in a fashion that greatly restricts the potential for those harms.
Acknowledgements

I am indebted to countless individuals and organizations who have supported me in various ways over the years it has taken me to write this thesis, but I must draw special attention and give thanks to the following:

To the Social Sciences and Humanities Research Council of Canada and the Faculty of Law at the University of Toronto, who graciously provided the funding that allowed me to complete this project.

To my supervisor, Lisa Austin, and the members of my committee, Trudo Lemmens and Ariel Katz, whose comments and feedback made this thesis a dramatically better piece of work than it would otherwise have been.

To my colleagues in the SJD programme, with whom I have had the immense privilege of sharing the many highs and lows of life as a graduate student. I expect big things from all of you.

To the incomparable Julia Hall, who was tirelessly helpful in aiding myself and the other graduate students as we navigated the maze of the University of Toronto bureaucracy and tried to seek out free food.

To the students, faculty, and staff at Osgoode Hall Law School, who provided me with the wonderful experience of teaching many bright minds over the last four years and helped remind me of the reason I originally wanted to study law.

To Laura, who I did not know when I began writing this thesis, but now with whom I cannot imagine life without.

Most of all to my parents, who have loved, supported, encouraged, criticized, and cajoled me in all the right amounts since the moment I was born, and in so doing have provided me with the platform from which everything good in my life flows.

Stuart Hargreaves

Toronto, Canada

May 26, 2013.
# Table of Contents

Abstract .......................................................................................................................... ii  
Acknowledgements ......................................................................................................... iii  
Table of Contents .............................................................................................................. iv  
List of Figures .................................................................................................................. vi  
List of Appendices .......................................................................................................... vii  

## Chapter 1: Introduction ................................................................................................. 1  
Introduction ...................................................................................................................... 1  
The Link Between Autonomy, Privacy, & Surveillance .................................................. 9  
*Autonomy, Privacy, & the Metaphor of the Boundary* .................................................. 9  
*Control-based Accounts of Privacy, Data Protection Regimes, & Surveillance* ....... 19  
Summary .......................................................................................................................... 23  

## Chapter 2: What are Geo-Immersive Technologies? ..................................................... 25  
Origins, Development, & Major Service Providers ......................................................... 26  
Usage Cases & Consumer Response .............................................................................. 37  

## Chapter 3: Understanding Geo-Immersive Technologies as a Surveillance Practice .... 49  
Surveillance Theories: Scrutiny for the Purpose of Influence ....................................... 49  
The Bifurcation of the Surveillance Architecture ......................................................... 57  
Unleashing the Human Flesh Search Engine .................................................................. 62  
*The Power to Identify* .................................................................................................. 62  
*The Viral Spread of Imagery* ....................................................................................... 67  
Summary .......................................................................................................................... 74  

## Chapter 4: The Potential Harms of Widespread Geo-Immersive Surveillance .......... 76  
Digital Shaming for the Violation of Real-World Norms .............................................. 76  
*Why Do Online Communities Seek to Enforce Norms Against Others?* ................. 85  
*The Online Disinhibition Effect* .................................................................................. 91  
*Sanctions Without Norm Transgression* .................................................................... 98  
*Is Geo-Immersive Surveillance Leading to Increased Social Sanctions?* ................ 103  
*The Possibility of Positive Norm Reinforcement* ....................................................... 105  
The Potential Effects on Behaviour & Norm Transmission ......................................... 107  
*Anticipatory Conformity* ........................................................................................... 109  
*The Potential for Panopticism & the Internalization of Norms* ............................... 119  
*The Public Harm of Norm Internalization* ................................................................ 126  
Summary .......................................................................................................................... 131  
A Legal Response: When, and Against Whom? ............................................................. 132  

## Chapter 5: Rethinking Autonomy & Privacy ................................................................. 139  
Reinterpreting the Metaphor of the Boundary: From Spatial to Dialectic Accounts ...... 140  
Relational Autonomy ...................................................................................................... 153  
Relational Privacy .......................................................................................................... 162  
Summary .......................................................................................................................... 170  

## Chapter 6: “Invasion of Privacy” Torts & Geo-Immersive Surveillance ...................... 172  
The Origin of Invasion of Privacy Torts – The American Context ................................ 173  
The Provincial Statutory Torts for Invasion of Privacy ................................................ 176
Potential Actions Under the Statutory Torts................................................................. 177
The New Ontario Common Law Tort for Invasion of Privacy ........................................ 188
Potential Actions Under the Newly Recognized (Ontario) Common Law Tort.................... 195
A Reconceived Tort...................................................................................................... 211
Lessons from Abroad .................................................................................................. 212
Other Options for Re-drawing the Boundary of the Tort................................................. 221
The Ineffectiveness of a Private Law Action as a Tool Against Mass Surveillance............ 226

Chapter 7: PIPEDA, the OPC, & Geo-Immersive Surveillance ....................................... 237
Are the Fair Information Principles Relevant in the Context of Surveillance? .................. 238
The Applicability of PIPEDA to Geo-Immersive Technologies........................................ 242
Are Geo-immersive Technology Providers ‘Organizations’?.......................................... 243
Are the Imaging Operations ‘Commercial Activities’?.................................................. 244
Do Geo-immersive Technology Providers Collect, Use, or Disclose ‘Personal Information’? 251
Geo-immersive Technologies & Section 5(3) of PIPEDA: Reasonableness ......................... 264
‘Appropriate’ Purposes & the Eastmond Framework...................................................... 265
Geo-immersive Technologies & the Substantive Requirements Under Schedule 1.............. 274
Knowledge & Consent................................................................................................. 274
Limiting Collection..................................................................................................... 287
Safeguards.................................................................................................................... 289
Summary....................................................................................................................... 293

Chapter 8: Reinvigoration of PIPEDA Through Relational Privacy ................................. 294
A More Robust Application of Schedule 1..................................................................... 294
Knowledge & Consent.................................................................................................. 296
Limiting Collection..................................................................................................... 299
Safeguards.................................................................................................................... 301
Summary....................................................................................................................... 307

Chapter 9: Conclusion ................................................................................................. 311
Geo-immersive Surveillance, Privacy, Autonomy, and the Law........................................ 311
Appendices.................................................................................................................... 320
Appendix 1 – The OECD Guidelines............................................................................... 320
Appendix 2 – The CSA Model Code Provisions.............................................................. 322
Bibliography................................................................................................................. 324
Legislation.................................................................................................................... 324
Jurisprudence............................................................................................................... 324
Office of the Privacy Commissioner of Canada Case Findings......................................... 328
Secondary Sources...................................................................................................... 331
List of Figures

Figure 1 – the Stanford CityBlock Project truck..............................................................27
Figure 2 – the second-generation Street View van.......................................................28
Figure 3 – the second-generation Street View imaging rig..........................................29
Figure 4 – the fourth-generation Street View imaging rig...........................................30
Figure 5 – the fourth-generation Street View car.......................................................30
Figure 6 – the Street View Trike................................................................................31
Figure 7 – the Street View Snowmobile......................................................................32
Figure 8 – the Street View Backpack.........................................................................33
Figure 9 – currently imaged zones for Google Street View.........................................34
Figure 10 – DIY Backpack..........................................................................................37
Figure 11 – DIY Roof-rack..........................................................................................37
Figure 12 – unsuccessfully blurred image...................................................................43
Figure 13 – woman and dog.......................................................................................44
Figure 14 – blurred faces............................................................................................45
Figure 15 – surveillance vs. sousveillance.................................................................45
Figure 16 – the Omniveillant Web..............................................................................60
Figure 17 – man urinating............................................................................................73
Figure 18 – topless sunbather.....................................................................................99
Figure 19 – vomiting man..........................................................................................101
Figure 20 – men and car............................................................................................102
Figure 21 – demographics of 4chan..........................................................................116
Figure 22 – image generated by Google Street View of southeast corner of Bay St. and King St., Toronto, Ontario........................................................................259
Figure 23 – driving locations in Canada......................................................................285
Figure 24 – driving locations in USA.........................................................................285
Figure 25 – removing pedestrians from Street View..................................................302
Figure 26 – summarization of the steps used to automatically anonymize a pedestrian within a generic cityscape image.........................................................304
List of Appendices

Appendix 1 – the OECD Guidelines........................................................................................................327
Appendix 2 – the CSA Model Code Provisions.........................................................................................329
Chapter 1: Introduction

Introduction

This thesis is about the interaction between privacy, autonomy, surveillance, the law, and social norms in the broader context of commercial mapping services that digitally record public spaces and render them accessible to anyone in the world with an Internet connection. Over the last half-decade, large corporations associated primarily with the ‘digital economy’ have begun to intensively fund and deploy an infrastructure of ‘geo-immersive technologies’ that form the backbone of such services. Even though the ‘imaging’ that occurs under these services is currently relatively infrequent, this is not likely to remain the case. While Google and Microsoft are perhaps the most well known operators of such systems, as the cost of the technology drops more and more players will enter the field, meaning imaging in the future is likely to be more frequent and more detailed as competition increases. This thesis is premised on the contention that if these new technologies are left essentially unregulated, the result will be regular exposure of those who are caught in the images to a global audience of potentially billions; a system, in effect, of ‘geo-immersive surveillance’.

There has been no sustained scholarly analysis of these technologies in either sociological or legal terms – this thesis is an attempt to fill that gap, offering a critical analysis and proposals for regulation. In so doing, it draws from theoretical literature across a number of fields and offers a doctrinal study of the applicable Canadian legal regimes. There is necessarily a large

---

1 I prefer ‘imaged’ from the more conventional ‘photographed’, as a way of distinguishing the unique operation of geo-immersive surveillance.
speculative element to this thesis – these technologies are new, and their effects remain uncertain. While it cannot be said that a complete geo-immersive surveillance system currently exists, I intend to nonetheless show that its early stages are already evident, and that pre-emptive regulation through existing data protection legislation is the best option for limiting the potential for associated social risks. In contrast to scholars who have argued that privacy (and thus privacy law) offers little in the way of remedying the harms of surveillance, I will argue that privacy law in the guise of the fair information principles does in fact offer a sufficient antidote for certain forms of commercial surveillance. I offer a concept of ‘relational privacy’ that is a means of justifying a more robust application of the fair information principles with the result, I claim, that geo-immersive surveillance can be regulated in a manner that adequately preserves the legitimate privacy interests Canadians have in public space, whilst allowing the continued development and use of an innovative set of technologies.

I will suggest that the infrastructure associated with these new geo-immersive technologies can be understood as being bifurcated between the parties that generate the images and the parties that peruse the images. While I do not ascribe any malicious intent on the part of the organizations that generate the images, I will argue that the possibility nonetheless exists for behaviour shaping thanks to the actions of third parties under this structure. I will go on to suggest that Panoptic-style processes may result in almost anyone living in a society characterized by regular geo-immersive surveillance suffering indirect social harms related to norm formation and transmission, even though they themselves may not be captured by the cameras. Such surveillance may retard capacities for meaningful reflection and deliberation, as
individuals subconsciously assume the socially dominant norms around them. These factors mean that a widespread deployment of geo-immersive surveillance systems ought to be interpreted as a broad threat to the autonomy of all those living in a society, not merely those who are directly subject to surveillance. Thus, I will argue that these new technologies can impinge upon the interests of even those who are not directly captured in an image.

Admittedly, this is the reason scholars have long criticized ‘privacy’ as an incomplete solution to the problems that can be caused by surveillance. Lyon, for instance, argued more than twenty years ago that the “stock response” of ‘privacy’ as the antidote to ‘surveillance’ issues was unhelpful, and “inadequate to cover what is at stake in the debate over contemporary surveillance.” I will consider this argument in more detail later in this Chapter, but this thesis ultimately argues that privacy (and privacy law) remains a valuable tool for regulating commercial surveillance. Privacy, after all, is a “broad, all-encompassing concept that envelops a whole host of human concerns about various forms of intrusive behaviour.” Solove similarly proposes that privacy interests can be seen as an interconnected web of things that are all related, though they may lack a single common central point. He therefore seeks to “map the typography” of a web of these interests by positing a taxonomy of four groups of “harmful activities” that can impinge upon privacy interests (or ‘create social disruption’) – invasion upon the person directly, information collection, information processing, and finally information

---

dissemination. I will show in this thesis that geo-immersive technologies effectively collect and process information about individuals captured in imagery, and subsequently disseminate it to others who would not otherwise have such access; it clearly makes sense to consider this as triggering a ‘privacy’ loss. I will also suggest, however, that widespread surveillance also results in the reduction of an individual’s ability to gauge their potential exposure to an audience when in public, and this too can be interpreted as a privacy loss – even if they are not actually captured in an image. The mere existence of the surveillance infrastructure alters our ability to calculate or accurately predict our exposure, even if we are not caught by the cameras. While surveillance scholars would argue that privacy laws cannot offer a remedy to individuals in such a scenario, I intend to argue that this is not necessarily true. I will suggest that if data protection laws can effectively regulate the collection of geo-immersive imagery ‘at source’, then the consequence is improved control over exposure for everyone. As a result, the concept of ‘privacy’ (and thus, privacy laws) can be seen as capable of controlling the growth of certain forms of commercial surveillance infrastructures in a manner that benefits even those not directly captured in an image.

My contention is that autonomy and privacy are closely linked and one’s approach to the former can colour one’s conception of the latter. I will suggest that it is conceptions of privacy based on an underlying approach to autonomy focused on the elimination of external influence that are more likely to struggle with regulating systemic forms of surveillance. I therefore consider theories of ‘relational autonomy’, drawn from feminist legal theory, suggesting that they offer a superior understanding how privacy claims ought to be seen as normatively valuable. Relational

---

autonomy perceives of privacy not as a ‘bubble’ that can be ‘popped’ by an unwanted invasion, but rather as a blanket that can surround both ourselves and those close to us. It can likewise be discarded at times, and can be both worn down and repaired by certain practices. This, I argue, may offer a more useful way of thinking about regulating surveillance of public space for commercial purposes through the vehicle of privacy law.

I will suggest that it is more plausible and practical as means of legal control of geo-immersive surveillance to focus on limiting the collection of imagery at source; that is, to focus the legal question on the actions of the geo-immersive service provider, rather than the ultimate users of the imagery. This thesis therefore considers two possible legal options to the regulation of geo-immersive technology providers – first, bringing an action against geo-immersive technology service providers for the tort of ‘invasion of privacy’, and second, relying on Canada’s data protection law, the *Personal Information Protection & Electronic Documents Act* (PIPEDA)\(^7\) to suggest that they have failed to follow the protections given to personal information collected for commercial purposes. My analysis indicates that existing judicial interpretations of invasion of privacy torts in Canada appear to rely heavily on a spatial approach to privacy, making a successful legal claim for invasion of privacy against a geo-immersive technology provider seemingly impossible to achieve. I therefore consider whether privacy torts could be based on a kind of ‘relational’ understanding, but conclude that private law actions generally are not the correct vehicle for regulating systems of geo-immersive surveillance. It is unlikely that an effective action could be crafted that would capture the operation of geo-immersive surveillance without also capturing a whole host of other innocuous ‘watching’ behaviours that occur in

---

\(^7\) *Personal Information Protection & Electronic Documents Act*, SC 2000, c 5 (‘PIPEDA’).
public spaces. Even if such a tort could be crafted, I suggest that private law remedies would still not be a suitable tool for regulating the kind of persistent, low-grade surveillance characteristic of geo-immersive technologies.

I therefore suggest that PIPEDA is a more suitable vehicle for advancing the goal of more tightly controlling geo-immersive surveillance, at least in part because it is not oriented around the same ‘spatial’ questions that invasion of privacy torts appear to be. I note that surveillance scholars have argued that ‘privacy as control’ regimes (such as PIPEDA) are only applicable where personal information is in fact collected, processed, or distributed, and therefore cannot adequately respond to the systemic harms that can accompany living in a ‘surveillance society’. However, I argue that the bifurcation of the surveillance infrastructure in the context of geo-immersive surveillance means that PIPEDA might nonetheless be a useful tool to regulate the collection of imagery ‘at source’. My analysis suggests, however, that the Office of the Canadian Privacy Commissioner’s (OPC) application of the ‘fair information principles’ as implemented under Schedule 1 of PIPEDA is, in the case of geo-immersive technologies, currently inadequate. I therefore propose a more robust application of the provisions of Schedule 1 that appear most relevant to the operation of geo-immersive technologies, justified through reference to the ideas of relational privacy introduced earlier. I conclude that by regulating the collection of imagery at source and applying to it a specific set of rules, the emergent geo-immersive surveillance infrastructure can be adequately controlled. This also strikes, I suggest, the proper balance between the legitimate privacy interests Canadians

---

8 The ‘fair information principles’ are the basis for data protection legislation in many countries; they originated in the OECD Privacy Guidelines, attached here as Appendix 1.
maintain while they in public areas and the freedom of organizations to develop innovative technologies that draw personal information from that same space. I do not seek to ban geo-immersive technologies, but rather only regulate them in a fashion that minimizes the possibility of any related serious social harms, whilst preserving them as the basis of many useful and innovative tools from which Canadians can benefit.

The ultimate conclusion of this thesis is that while geo-immersive surveillance is a new and potentially risky phenomenon, the necessary legal tools for its adequate regulation already exist in Canada. This is true despite long-standing criticisms of ‘privacy’ (and thus, ‘privacy law’) as an insufficient response to the dangers of surveillance. I contend that privacy laws grounded in the fair information principles can, in fact, successfully constrict the collection of imagery and thereby significantly reduce the prospect of broad social harms arising from its subsequent distribution. Considering privacy in ‘relational’ terms offers a useful method of bypassing the traditional public/private dichotomy that underpins the traditional privacy law scholarship in a way that responds better to the kinds of concerns raised by low-grade, systemic public surveillance for commercial purposes, and helps to justify a more robust application of the fair information principles by the OPC than is currently the case. I suggest, then, that reinvigoration of the relevant fair information principles in a way that reflects the commitments of relational privacy has the potential to prove an effective method of controlling the sources of geo-immersive imagery without eliminating the technology as a useful tool. Adequately reconstructed and applied, ‘privacy law’ may in fact be a sufficient antidote for geo-immersive surveillance. I also acknowledge, however, that there do remain limits to the effectiveness of
privacy law in this area. For instance, the remedies I propose would not hold salience if a true ‘peer-to-peer’ surveillance system arose that was not characterized by the bifurcated structure between commercial collectors and non-commercial viewers in the manner geo-immersive technologies are. This thesis is about a specific set of legal solutions to a specific kind of problem – the unregulated spread of technologies that digitally map public space for commercial purposes.

While I will go on in subsequent chapters to consider each of the above arguments in greater detail, in the rest of this first chapter I wish to offer a brief account of the connection between autonomy and privacy. At the outset, it is important for me to acknowledge that privacy is held to further (or at least is held to have the potential to further) many different values, and these values are likely to fluctuate over time and through different cultures – I am not trying to develop a ‘single’ theory of privacy that is universally applicable. Indeed, as Gavison acknowledged in her review of the literature, privacy has been linked to many individual goals including intimacy, creativity, human relations, freedom from physical access, personal growth, liberty of action, and mental health; indeed, it has so many possible claims that she quipped that it “appears that privacy is central to the attainment of individual goals under every theory of the individual that has ever captured man’s imagination.”\(^\text{9}\) However, I do want to pay special attention to the concept of privacy furthering autonomy, which is a recurring theme in much of the literature. In the next section, then, I explore the link between privacy, autonomy, and surveillance more closely.

\(^{9}\) Ruth Gavison, "Privacy and the Limits of Law" (1979) 89 Yale LJ 421 at 445.
The Link Between Autonomy, Privacy, & Surveillance

Autonomy, Privacy, & the Metaphor of the Boundary

Autonomy plays an important role in the liberal tradition, in which “to be autonomous is seen by many as the very core of a valuable human existence.”\footnote{10} The autonomous actor lies at the heart of liberal individualism writ large, centred primarily around the rational, rights-bearing citizen pursuing her interpretation of the good life. Anderson and Honneth identify autonomy as one of liberalism’s “core commitments”, tracing it to the early modern period of European history during which, they argue, individuals increasingly abandoned social and community bonds in pursuit of their own goals.\footnote{11} Yet despite (or perhaps because of) its importance to broad liberal political theory, it remains a contested concept.\footnote{12} Indeed, there is probably no universal ideal of ‘autonomy’, but rather “one concept and many conceptions.”\footnote{13} However, Christman notes that while there may indeed be multiple ways to approach autonomy in terms of defining its boundaries, functions, or effects, its conceptual core is that to be autonomous is to have the psychological ability of self-governance.\footnote{14} Dworkin concurs, seeing the shared element of diverse approaches to autonomy as a “certain idea of persons being self-determining.”\footnote{15} Indeed, the etymology of the word itself points to the abstract notion that underpins it: derived from the

\footnote{12} Paul AB Clarke, \textit{Autonomy Unbound} (Aldershot, UK: Ashgate, 1999) at 11.
\footnote{14} Christman, \textit{supra} note 10 at 5.
Greek roots of *autos*, meaning ‘self’, and *nomos*, meaning ‘law’ or ‘rule’, autonomy’s literal meaning therefore is ‘the having or making of one’s own law’.\(^{16}\)

The notion of autonomy still finds its core meaning in the idea of being one’s own person, directed by considerations, desires, conditions, and characteristics that are not simply imposed externally on one, but are part of what can somehow be considered one’s authentic self.\(^{17}\)

Dworkin believes that autonomy can be thought of (and used) as a moral, political, or social ideal.\(^{18}\) Morally, it suggests that there is some benefit to having individuals choose or adopt their own moral code, and so individuals ought to have the capacity to subject themselves to objective moral principles. Politically, it can be used as a means of arguing against any kind of institutional composition that attempts to impose upon citizens a particular set of ends or values. For example, democratic mechanisms consistent with the value of autonomy likely do not depend on conformity with a particular religious or cultural tradition before allowing participation. Socially, it can be thought of as the idea that one has the ability to choose one’s own conception of the good life—Christman, for example, describes personal autonomy as a “morally neutral trait that individuals can exhibit relative to any aspects of their lives”\(^{19}\), while for Raz it is “the vision of people controlling, to some degree, their own destiny, fashioning it through successive decisions.”\(^{20}\)


\(^{18}\) Dworkin, *supra* note 15 at 10-11.

\(^{19}\) Christman & Anderson *supra* note 17 at 2.

Christman and Anderson suggest that in order for the individual to achieve ‘autonomy’ or be able to govern oneself, what is required is that the individual be able to “act competently” and that those actions stem from desires that are their own. In turn, this requires that two sets of conditions – ‘competency conditions’ and ‘authenticity conditions’ – be met. To meet the competency conditions, they claim an individual must have the capacity for rational thought, self-control, and self-understanding, as well as being free from coercion in exercising those capacities. Meeting the authenticity conditions requires the capacity to reflect upon and endorse one’s desires, values, or wishes. Such procedural autonomy can be seen as something approaching an equation of independence (meaning a lack of overt coercion) plus the ability for self-reflection. Dworkin too suggests an account of autonomy based on ‘procedural independence’, which for him is composed of two things. First, that the individual be free from manipulation or deception in the arrival of their ‘first-order’ desires (those simple desires to do or not to do things – a wish to travel, a desire to marry, a decision to work as a teacher instead of as a nurse, etc.). Kupf describes such first-order considerations as those that underlie the decisions that “occupy us in the ordinary course of life.” The second (and crucial) element for Dworkin is the existence of ‘second-order’ actions, or those that are used to reflect upon first-order desires; these second-order capacities parallel the authenticity and competence conditions mentioned above. Second-order actions or judgments involve a degree of critical self-reflection, in which individuals consider the implementation of their first-order desires.

This process of consideration enables them to choose which first-order desires to follow and

21 Christman & Anderson, supra note 17 at 3.
22 Ibid.
23 Ibid.
24 Dworkin, supra note 13 at 20.
which ones to reject, and in what order. For Dworkin, the key element of autonomy is this critical reflective capacity, along with a secondary capacity to change or at least attempt to change those first-order desires in light of the higher-order reflection. Crittenden also suggests that to be “self-rulled, one must be able to step back reflectively from her social context to evaluate critically the norms and standards and ends of that context.” By reflecting in this manner, “persons define their nature, give meaning and coherence to their lives, and take responsibility for the kind of person they are.” Richards concurs, suggesting that “autonomy is a complex assumption about the capacities… of persons, which enable them to develop, want to act on, and act on higher-order plans of action which have as their self-critical object one’s life and the way it is lived.” These procedural accounts of personal autonomy depend upon a continual process of self-evaluation and self-criticism in light of the available information, unhindered by outside forces. Only this process, it is claimed, can lead to truly autonomous activities. All these interpretations share, however, “a notion of the self which is to be respected, left unmanipulated, and which is in some way independent and self-determining.” So while there are unquestionably different ways of thinking about autonomy, for the purposes of this thesis I wish to consider it in the sense of ‘personal’ autonomy, and I therefore adopt Friedman’s succinct description that “personal autonomy involves acting and living accord to

26 Dworkin, supra note 13 at 20.
28 Dworkin, supra note 13 at 20.
30 Dworkin, supra note 13 at 12.
one’s own choices, values, and identity, within the constraints of what one regards as morally permissible.”

In my view, this consideration of personal autonomy integrates much of the normative content privacy is commonly held to further or protect – and indeed, there is a deep link between the two. The idea that certain forms of privacy can help protect or promote ‘personhood’ or the self-development necessary for an individual to function properly is well recognized. Indeed, in their oft-cited law review article, Warren & Brandeis advocated for a right to privacy in order to protect what they described as the individual’s ‘inviolate personality’. While they did not explicitly define what this personality was, it is suggestive of some vital core of the self. A number of privacy scholars agree with this general notion, though not necessarily using the same phrasing, or entirely agreeing on what precisely the ‘core’ of a person is. Bloustein, for instance, believes that ‘inviolate personality’ is “the individual’s independence, dignity and integrity [which] defines man’s essence as a unique and self-determining being” and that “this is in some sense a spiritual interest rather than an interest in property or reputation.” Fairfield suggests that privacy secures us against “unwanted intrusions into areas of life that… profoundly touch on who we are and what meaning our lives hold for us.” Schoeman also believes that, in general, the protection of the self is a desirable thing and that privacy “marks

---

out something morally significant about what it is to be a person.”

He argues that privacy allows individuals to express the different dimensions of the self, not in the sense of multiple-personality disorders, but rather in the sense that behaviour is not consistent, and shifts across contexts. Austin, too, argues “we require some respite from the public gaze” not only so that we may act in unconventional ways, but simply in order that we can gather ourselves and subsequently put forth the desired public face.

Retaining the ability to withdraw from public gaze is one method of ensuring a “zone that permits unconstrained, unobserved, physical and intellectual development... a zone that furnishes room for critical, playful subjectivity to develop.” This zone provides the intellectual and emotional space for us to choose which activities or thoughts we wish to share or account for, and which we prefer to keep private, whatever the reason. In the same way, this zone helps us at a base level ‘be who we want to be’, allowing us room to consider our options before we act; it is much harder to ‘gather one’s thoughts’ when being subject to a persistent gaze. There is an intimate connection between this space for reflectivity and self-development, which can be hampered in the face of intense social pressure. As Bloustein argues,

The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy, or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the

---

36 Ibid.
37 Lisa M Austin, "Privacy and the Question of Technology" (2003) 22 Law & Phil 119 at 147. Austin also notes the limits to this approach, arguing elsewhere that “it is one thing to argue that we need some respite from the public gaze in order to forge an authentic self, but is quite another to assert that the particular gaze of a particular other in fact interferes with this project of authenticity”; see Lisa M Austin, "Privacy and Private Law: The Dilemma of Justification" (2010) 55(1) McGill LJ 1 at 34.
mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man. Such a being, although sentient, is fungible; he is not an individual.  

It is often posited that privacy can assist in such self-development processes by allowing individuals the freedom and space to ‘grow into’ themselves. Moore, for example, argues that privacy is a “cultural universal necessary for our proper functioning.” For Reiman, it is “a social ritual by means of which an individual’s moral title to his existence is conferred,” and by this I take him to mean that privacy helps individuals understand that some aspects of the self are theirs and theirs alone, and this understanding is key to an individual seeing themselves as, in fact, an ‘individual’. He goes on to argue that individuals “must recognize that [they] have exclusive moral rights to shape [their] destiny,” and privacy violations therefore are those that “penetrate the private reserve of the individual” and “[destroy] the Self.” Wasserstrom concurs, suggesting that one plausible conception of what it is to be a person is “the idea of an existence of a core of thoughts and feelings that are a person’s alone,” and so enforced disclosure of these thoughts and feelings diminishes personhood; privacy protects against such disclosure.

Liberalism traditionally conceptualizes autonomy and privacy in similar ways. The traditional liberal view of autonomy, for instance, is that it “increases with the reduction of restrictions, [so]

39 Bloustein, supra note 33 at 188. 
42 Ibid. 
individuals realize their autonomy by gaining independence from their consociates.”

Fairfield argues that “as a philosophy committed to human freedom, one of liberalism’s principle concerns is to safeguard private life from undue intrusions by public institutions.” Such an approach sees personal autonomy as a quality held by the rational actor, able to act free from outside influences in considering his or her options, determining which of those is the most suitable vehicle for advancing their primary desires, and then acting successfully upon that determination. The result is the creation of a ‘barrier’ or ‘zone’ that protects the individual from the encroachment of the collective:

The traditional concept of autonomy sets it in opposition to collective power, to shield individuals from the collective, to set up legal barriers around the individual that the state cannot cross.

Under this school of thinking, as Nedelsky dryly notes, “the most perfectly autonomous man is the most perfectly isolated.” For classical liberals, the protection of individual autonomy is therefore “to be achieved by erecting a wall of rights between the individual and those around him.”

This ‘autonomy as independence’ also informs conventional liberal approaches to privacy, with the result that privacy rights are frequently conceptualized as a protective barrier. Lyon argues, and I accept, that the “liberal approach… tends to conflate privacy with resisting intrusion”; this also describes the conventional liberal approach to autonomy. For Bennett, “philosophically, privacy has its roots in liberal individualism, and notions of separation between the state and

---

44 Anderson & Honneth, supra note 11 at 128.
45 Fairfield, supra note 34 at 5.
47 Ibid.
48 Ibid.
49 Lyon, supra note 2 at 186.
civil society.”

Thus, much as a conception of autonomy as independence tends to lead to a focus on shielding the individual from external restraint through a wall of rights, liberal accounts of privacy have also been based primarily on the idea of a legal barrier protecting the individual from improper interference or access. As Stadler describes it, privacy viewed in this fashion resembles a “kind of bubble that surrounds each person, and the dimensions of this bubble are determined by one’s ability to control who enters and who does not. Privacy is a personal space; space under the exclusive control of the individual.”

Nedelsky also sees privacy as being “closely associated with [a] boundary image.”

Boundary approaches can be understood as seeing privacy primarily as ensuring the ability of the individual to ‘withdraw’, or to be shielded from unwanted intrusions. Warren & Brandeis’ seminal article on privacy in the American legal system advocated for a right to privacy that protected an individual’s right to be “let alone”, which can be understood at least partially as a claim to solitude, a right to a barrier that can separate the individual from the collective. I will suggest in this thesis that the Canadian courts, when faced with claims for invasions of privacy in the civil context, appear to approach privacy primarily from this perspective. The result is that one’s location during the alleged improper watching is the dominant factor in the success or failure of the claim – claims made in ‘public’ are doomed to fail. Effectively, by being in public

51 Felix Stalder, "Privacy is Not the Antidote to Surveillance" (2002) 1(1) Surveill Soc 120 at 121, cited in Bennett supra note 50 at 488.
53 This is not necessarily the case in the criminal context, however, in which the courts have accepted that individuals in public space retain privacy interests vis-a-vis agents of the state. See for instance R v Ward, 2012 ONCA 660, in which Doherty JA (for the court) argued “surely, if the state could unilaterally, and without restraint, gather information to identify individuals engaged in public activities of interest to the state, individual freedom and with it meaningful participation in the democratic process would be curtailed” (at para 74).
space, the individual has chosen engagement over withdrawal, and therefore has relinquished their expectation of privacy. This is an approach to privacy grounded in a spatial distinction between what is private and what is public and is indicative, in my view, of an underlying approach to autonomy that is consistent with the traditional liberal view of ‘autonomy as independence’.

Certainly, conceptions of privacy reliant upon this boundary idea and its associated public/private spatial dichotomy have faced numerous critiques – equating privacy with purely solitude has long been understood to be an impoverished vision. Regan, for example, argues that “the philosophical basis of privacy overemphasizes the importance of privacy to the individual, and fails to recognize [its] broader social importance.”54 She suggests that since people’s lives are necessarily both public and private, the two “should not be seen as antithetical.”55 Allen similarly suggests that a dichotomous public/private approach to privacy view ignores that individuals live “lives enmeshed in webs of accountability for conduct… we are accountable for private conduct to [both] government and non-government actors.”56 As a result, she rejects the idea that privacy creates a zone of conduct for which we are not accountable (i.e., that which is private), and in doing so wants to break down the barrier that some place between public and private life. Bennett also finds that a boundary approach to privacy “reifies a problematic distinction between the realms of the public and the private.”57

57 Bennett, *supra* note 50 at 486.
Gilliom meanwhile suggests that privacy’s “roots in individualism mean that [it] no longer reflects the complexity and interdependence of our world.” Solove too acknowledges “privacy is more complicated” than a division between public and private, and “modern technology poses a severe challenge to [this] traditional binary understanding of privacy.” Stalder has also rejected the boundary approach as something that just “doesn’t work.” Indeed, the criticisms are long-standing and widespread, to the point where Bennett concludes that the individualistic approach associated with a dichotomous public/private barrier no longer “constitute[s] a paradigmatic understanding of the problem.” Yet, while the academe may have in large part rejected this dichotomous approach to privacy, this thesis will demonstrate that it does not yet appear to have infused the work of the Canadian judicial system, at least in the context of tort claims for invasion of privacy.

Control-based Accounts of Privacy, Data Protection Regimes, & Surveillance

I will also suggest in this thesis that nothing in the text of Canada’s data protection law indicates it is dependent on a spatial orientation to privacy claims, and thus it may be a better vehicle for preventing the harms that may be caused by geo-immersive surveillance from arising. PIPEDA is rooted in what might be described as a ‘control’ approach to privacy – one in which the individual is given particular rights to control the collection, use, and distribution of her personal information, subject to certain counterbalancing concerns. Control-based privacy theories are often associated with Westin, who argues that “privacy is the claim of individuals, groups or

---

60 Stalder, supra note 51 at 121.
61 Bennett, supra note 50 at 487.
institutions to determine for themselves when, how and to what extent information about them is communicated to others."  

Likewise for Parent, privacy is “the condition of a person’s having undocumented personal information about herself not known to others” and ‘undocumented information’ is information that is “not part of the public record and as such unavailable for public inspection.”  

Fried suggests that privacy “is not simply the absence of information about us in the minds of others; rather it is the control we have over information about ourselves” [emphasis in original].  

Miller thinks “the basic attribute of an effective right of privacy is the individual’s ability to control the circulation of information relating to him.”

Control theories of privacy have gained greatest traction in legal instruments designed to protect individual privacy in the commercial context. Thus, while a legislative regime based upon control of information would likely seek to restrict a hotel asking its guests about their religious beliefs or sexual preferences upon check-in, it would have nothing to say about the regulation of ‘gossip’ about those same topics in a non-commercial context. Of course, a legal privacy regime based upon control over information could still not be based on an absolute right of the individual to control all information circulating about them in a commercial context – this would be unworkable; particularly if “transposed into the commercial realm, it would undermine major industries and highly expedient government practices.”

Data protection regimes therefore generally limit the right to control information in two broad ways – first, by

---

64 Charles Fried, "Privacy" (1967) 77 Yale LJ 475 at 482.
limiting it to that which is classified as ‘personal’ information. In the case of PIPEDA, for instance, it is defined as “information about an identifiable individual.”67 Second, there is no absolute right to control granted over that information – data protection regimes are ultimately aimed at balancing off the privacy rights of individuals with organizational interests in the collection, use, or disclosure of personal information. For example, PIPEDA’s purpose is stated to be:

[To] establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.68

This suggests an alternative approach to limiting privacy claims that is not necessarily dependent on spatial or boundary questions, and therefore may be a more compelling option for the regulation of geo-immersive surveillance. Flaherty, for instance, has argued that “data protection law is implemented to limit [data-based] surveillance by other persons and organizations and thus to preserve individual privacy.”69 What I intend to show is that even though geo-immersive surveillance is a ‘visual’ form of surveillance, because it is dependent upon the distribution of information before the potential for scrutiny can occur, control regimes and data protection are useful mechanisms of regulating certain aspects of it.

However, as I noted earlier, privacy and privacy laws have long been called inadequate to the task of controlling surveillance, because the harms of surveillance extend beyond individual

67 PIPEDA, s 2(1).
68 PIPEDA, s 3.
69 Flaherty, supra note 3 at xiv.
privacy invasions. The inadequacy of privacy in the face of surveillance is a popular refrain in the literature. Lyon, for instance, has argued that “privacy alone falls far short as a means of challenging contemporary surveillance [because] it answers to personal fears of invasion and violation.”\textsuperscript{70} Stalder argues that surveillance issues must be understood in terms far broader that “individual transgressions of privacy.”\textsuperscript{71} Karas concludes that a “reliance on privacy rights is unlikely to effect the pervasive data collection” that characterizes many surveillance practices.\textsuperscript{72} Gray believes that “the effects of pervasive surveillance stretch beyond issues related to privacy.”\textsuperscript{73} Gilliom contends that it is necessary to “set aside the presumption that privacy” is the relevant issue in the context of surveillance practices.\textsuperscript{74} Ericson & Haggerty argue that “metaphors about privacy being invaded are not helpful” in helping us to understand the impact surveillance may have.\textsuperscript{75} Gray contends that “the effects of pervasive surveillance stretch beyond issues related to privacy.”\textsuperscript{76}

The criticisms, then, are in large part that surveillance is often not about lost control over information, and that surveillance harms extend beyond the individual. I accept that these criticisms are valid, however I intend to argue that there is nothing within the fair information principles or a legislative effort at granting control over personal information that ought to

\textsuperscript{71} Stalder, supra note 51 at 123.
\textsuperscript{72} Stan Karas, "Enhancing the Privacy Discourse: Consumer Information Gathering as Surveillance" (2002) 7 J Tech L & Pol'y 29 at 57.
\textsuperscript{74} Gilliom supra note 58 at 124.
\textsuperscript{76} Gray, \textit{supra} note 73 at 318.
preclude an approach to privacy that takes better account of its social value. In other words, a regime that attempts to protect privacy by granting an *individual* control over their personal information need not necessarily be underpinned by an *individualistic* understanding of the function of that privacy. Moreover, when confronted with a surveillance system characterized by a bifurcated infrastructure (as is the case with commercial street surveillance), the fair information principles may in fact be sufficient to control the collection of personal information in a way that dramatically constricts the possibility of broad social harms from arising. As a result, even though data protection legislation based upon the idea of control (and thus ‘privacy’) is often critiqued as being an insufficient antidote to surveillance, this may actually not be universally true; I conclude that the fair information principles continue to have relevance even in the context of certain forms of modern commercial surveillance.

**Summary**

I have argued in this chapter that there is a fundamental link between an approach to privacy that is based upon the metaphor of the boundary and an approach to autonomy that sees it primarily in terms of ‘independence’. I have suggested laws grounded in such an approach to privacy can struggle to respond to claims for privacy in public, because they tend to view privacy as the power to withdraw. I have also introduced the idea that even though data protection legislation based on theories of ‘control’ are often also seen as means of protecting the ability to withdraw, this need not be the case. I intend to show in this thesis that data protection legislation based on the fair information principles may in fact offer a plausible means of regulating commercial public street surveillance in a way that both adequately protects the legitimate privacy interests of Canadians whilst also creating space in which innovative
technologies can develop. While I will return to all of these ideas in later Chapters, for now I want to step back and consider the nature of geo-immersive technologies. In the next two Chapters, then, I explain in greater detail the way in which they operate, why they ought to be understood as forming the basis of an emergent surveillance practice, and the potential social harms that might accompany them should they remain effectively unregulated.
Chapter 2: What are Geo-Immersive Technologies?

Geo-immersive technologies are a set of nascent services that digitally photograph or otherwise record elements of public spaces, and then recreate them online in a manner that is accessible to anyone with an Internet connection. Typically, the images are collected by a camera attached to the roof of a car that drives along a pre-determined route, automatically taking digital photographs at regular intervals. The images are then processed into a format that allows a user, located anywhere in the world, to access a website and ‘walk through’ a recreation of the public space that had been digitally imaged. It is this ‘virtually walkable’ aspect that distinguishes geo-immersive technologies not only from conventional mapping, but also from other maps that are accessible online. While there are other online services that provide digitally depicted roads, streets, parks, and terrain in a manner similar to what one would find in a traditional paper map, and still others that complement traditional maps with sets of images taken of specific places in public, geo-immersive technologies are something different. The combination of the ability to ‘walk through’ a virtual recreation of a real-world place along with a more complete approach to image capture distinguishes geo-immersive technologies from both ‘standard’ online maps and also precursor systems like Amazon’s ‘A9 Maps’, which captured street-level images of businesses for its online directory.\textsuperscript{77} By collecting and processing massive amounts of visual imagery, providers of geo-immersive technologies are able to stitch together virtual recreations of public spaces that can be fully explored online with a field of view approaching 360 degrees.

The images are taken without regard to what is captured by the camera – a geo-immersive

system simply intends to recreate the world as it is captured, ‘warts and all’; importantly, this includes the digital capture of images of individuals who happen to be present when the car drives by. Whether the images are of murder victims,\textsuperscript{78} of sexual intimacy,\textsuperscript{79} of muggers,\textsuperscript{80} of a man dressed as a horse,\textsuperscript{81} of a woman urinating,\textsuperscript{82} or of a girl pretending to be run over by a car,\textsuperscript{83} in a few short years, geo-immersive technology services have already captured a wide swath of human behaviour in public. Before considering the impact that increased capture of this type of imagery is likely to have, it is useful to outline some of the basic technical and operational aspects of geo-immersive technologies.

**Origins, Development, & Major Service Providers**

The most well-known provider of a geo-immersive experience is Google, with its “Street View” service; indeed, Street View is perhaps the paradigmatic example of geo-immersive technologies, and it is to Street View that I will frequently refer throughout this thesis as a stand-in for all geo-immersive services. Street View began life as “The Stanford CityBlock Project”, part of the doctoral studies of several students at the Stanford (University) Computer Graphics Laboratory. The goal was to demonstrate the feasibility of “summarizing in a single image the extended linear architectural fabric seen at eye level along a possibly curving or turning street,

and doing so without introducing excessive distortions.” The initial technology demonstration involved students riding in the back of a pick up truck with a digital camera (see Figure 1), along with development of a software algorithm to knit the resulting images into a single viewable ‘world’. Google funded the initial project, and following a successful technology demonstration the team behind CityBlock was hired as part of the team working on Google’s online mapping service.

Figure 1 – The Stanford CityBlock Project Truck.

The imaging rig Google uses for Street View (understood as having three components – (1) an imaging device, mounted to (2) a vehicle, and connected to (3) a computer) has since evolved considerably, going through four phases. The initial prototype of the rig was considerably more advanced than the CityBlock Project Truck – Google mounted cameras, lasers, and a GPS to

---

86 Global positioning system – a device that can accurately calculate its position anywhere on the planet by reference to orbiting satellites.
the roof of a large sport-utility vehicle with several computers inside. This resulted in the collection of enough “compelling” imagery that the broader Street View project was green-lit by Google and large-scale public data-collection began in 2007.87 The second generation of the rig was a van (see Figure 2) equipped with side and front facing laser scanners, two high speed video cameras, eight high resolution still cameras in a rosette configuration (Figure 3), and multiple computers that recorded 500 megabytes of data per second while the vehicle was in motion. The van was equipped with a custom-built sensor system in each axle that assisted the computer in determining how an image should appear when it was taken as the vehicle was turning.88

![Figure 2](http://maps.google.com/intl/en_us/help/maps/streetview/images/photos/streetvan.jpg) – the second-generation Street View Van.89

88 Ibid.
While the van was successful in gathering imagery of several major US cities, Google concluded that it was too expensive to be scaled up into a nationwide or global imaging project. As a result, the third-generation rig was built using off-the-shelf components, using lower resolution cameras and a single laptop PC, and used the existing anti-lock braking system in the car to provide the directional inputs previously provided by the custom axle. This allowed for “cost savings and reliability, but at the cost of high quality imagery.” The fourth-generation of the rig therefore focused on improving the imaging components – Google developed a custom panoramic camera system they called the “R5”, featuring a rosette of eight 5-megapixel cameras, plus a fish-eye lens on top that captures images of the upper levels of buildings (see Figure 4). The fourth-generation system also used a custom car mount that allowed the camera to be raised and lowered, and featured three laser scanners allowing for the capture of three-dimensional data of the area. The vehicle the system was mounted on has captured the majority of the images on Street View today (see Figure 5).

---

91 Anguelov et al., supra note 87 at 33.
92 Ibid.
93 Laser range finders can create rough three-dimensional maps of an area by measuring the distance the laser travels before bouncing back off an object. See for example Huijing Zhao and Ryosuke Shibasaki, “Reconstructing
Figure 4 – the fourth-generation Street View imaging rig.95

Figure 5 – the fourth-generation Street View car.96

---


A fifth-generation of the rig is currently under development and will be based around another new camera, the “R7”, said to have 15 high-cameras over “an increased field of view [allowing users to] see down sidewalks, even on narrow streets.”97 In addition to the automotive-based rigs described here, Google has also attached imaging equipment to other vehicles in order to gain access to areas not served by roads. This includes a pedalled tricycle (see Figure 6) to record pedestrian routes and tourist attractions, and a snowmobile (see Figure 7) first used to record images at the Vancouver Olympics and subsequently popular ski resorts.98

Figure 6 – the Street View Trike.99

97 Anguelov et al., supra note 87 at 34.
98 Ibid.
In 2012, Google launched a system light enough to be carried by one person (see Figure 8), in order to allow hiking trails and other pedestrian-only areas to be mapped.

---

Future versions of Street View will combine the street-level imagery data with commercially available satellite imagery, allowing Google to create a “single three-dimensional model of a building that has high resolution facades as well as rooftops and back sides, enhancing the user experience of a walk-through.”

Beginning with imagery of major US metropolitan cities, Street View has now captured panoramic imagery in hundreds of cities, in twenty different

102 Anguelov et al., supra note 87 at 37.
countries, across four continents. Figure 9 represents Google’s estimate of where they have conducted public street surveillance operations, as of August 2012. The blue areas represent those areas that have been mapped by the Google Street View cars at least once. Google provides no information as to how often they re-photograph areas, or whether certain areas are subject to more frequent updates than others.

![Map of Street View availability](image)

**Figure 9** – Currently Imaged Zones for Google Street View.

While Google remains the dominant player, competing geo-immersive technology services are proliferating at a notable pace. The only competitor to Street View in Canada thus far is Canpages, and while it has recorded images for both Vancouver and Toronto, at the time of

---


writing only the Vancouver images were accessible online.\textsuperscript{105} Other major North American players include Microsoft and MapQuest. Microsoft launched a rival project to Street View known as ‘Streetside’ in late 2009, incorporating it into its existing online mapping service ‘Bing Maps’.\textsuperscript{106} While it currently features imagery of only 56 US metropolitan areas, Microsoft has stated its intention to expand coverage internationally at some future date.\textsuperscript{107} Meanwhile, also in late 2009, MapQuest launched a similar service covering 30 US cities and 15 suburbs (with no stated plans for international expansion), called 360\textdegree View.\textsuperscript{108}

Outside North America, there are also multiple locally focused geo-immersive providers.\textsuperscript{109} In Argentina, both Mappolo\textsuperscript{110} and Fotocalle\textsuperscript{111} offer imagery of Buenos Aires. In China, city8\textsuperscript{112} provides a similar service for Beijing, while the State Bureau of Surveying and Mapping’s own Map World\textsuperscript{113} covers a variety of Chinese cities at street level, in addition to offering satellite imagery of various global locations. In Germany, Sightwalk\textsuperscript{114} covers eight major metropolitan

\textsuperscript{109}Language barriers make it difficult to retrieve specific details about the technical operation of these services, though rough exploration of the provided links confirms that they do provide some kind of geo-immersive experience.
\textsuperscript{110}See \url{http://mappolo.com}.
\textsuperscript{111}See \url{http://fotocalle.com}.
\textsuperscript{112}See \url{http://city8.com}.
\textsuperscript{113}See \url{http://www.tianditu.cn/map/index.jsp}.
\textsuperscript{114}See \url{http://sightwalk.de}. 
areas. In Japan, Location View covers over 30 cities; it is paid service that features high-resolution video imagery, rather than conventional still photography. In Latvia, 1188.lv provides imagery of Riga. In Poland, Zumi covers multiple locations. In Romania, NORC offers imagery of 11 Romanian cities as well 14 non-Romanian locations. In Russia, Gdeetotdom offers imagery of 62 cities, Yandex offers imagery of 7 Russian and one Ukrainian city, and ru09 offers imagery for three Russian cities. Daum covers multiple South Korean cities. In Sweden, Hitta offers coverage of 29 cities and Eniro covers eight cities and three winter resorts. In Switzerland, GlobeVision offers street level video imagery in many Swiss cities, and has plans to expand internationally.

The price of geo-immersive technology has dropped so significantly during the time I have been writing this thesis that I am constantly required to update its technological elements; one such development has been the recent (June 2012) release of a ‘do-it-yourself’ geo-immersive kit. Available for purchase online for roughly $500, the kit can be carried either by a person using a backpack mount (see Figure 10) or can be attached to a car using a supplied roof-rack kit (see Figure 11). In the future, then, we are likely to see geo-immersive technologies deployed by small organizations or individuals.

116 See http://www.1188.lv/karte360/.
117 See http://zumi.pl.
119 See http://gdeetotdom.ru.
120 See http://www.yandex.ru.
121 See http://ru09.ru.
122 See http://www.daum.net
123 See http://hitta.se.
124 See http://eniro.se.
It comprises all the same elements of a geo-immersive system (camera, imaging processor, GPS), allowing individuals to create geo-immersive worlds of their neighbourhoods or anywhere they wish to travel. I have not yet been able to discover any publicly available imagery generated by these new DIY systems other than that generated by the seller of the kit for advertising purposes, but surely it is not far off. Again, the fact that large corporations currently dominate the geo-immersive space is no reason to expect that this state of affairs will remain permanent – more organizations will enter, collecting more imagery, and the frequency and likelihood of individuals being caught by the camera in this way will surely increase.

Usage Cases & Consumer Response

---

While Street View has been an undoubted success for Google and, as indicated, remains the leading player in the geo-immersive technology industry, it has also met pockets of resistance as it has expanded. Citizens in an English village responded to the photography of their neighbourhood by physically blocking the path of the Street View car.\textsuperscript{129} Public outcry in Japan forced Google to retake all its street level imagery at a lower height, after the first images were high enough to view over the fences that customarily surround Japanese homes.\textsuperscript{130} Public complaints in the Czech Republic\textsuperscript{131}, Germany,\textsuperscript{132} and Austria\textsuperscript{133} led to Street View being temporarily suspended until compromises were reached with public authorities over the process that would be used. Complaints in Greece\textsuperscript{134} apparently have not yet been resolved.

These reactions appeared to stem from a reflexive sense that the broad recording of public spaces is in some way an invasion of privacy. Indeed, initially Google did not build any privacy protections into its service – the images, once digitally sewn together, were otherwise unmodified before being made available to viewers online. Individuals who identified

\begin{itemize}
  \item \textsuperscript{133} “Google Bows to German Data Privacy Demands”, Der Spiegel, Jun 18, 2009, online, http://www.spiegel.de/international/germany/0,1518,631149,00.html, accessed Aug 14, 2010.
  \item \textsuperscript{132} “Austria ends ban on Google Street View; Google unmoved”, Search Engine Land, Apr 25, 2011, online http://searchengineland.com/austria-ends-ban-google-street-view-74518, last accessed Mar 17, 2013.
\end{itemize}
themselves in the images could request that they be deleted, but only after the fact. While that option still exists, in response to public complaints Google agreed to automatically blur licence plates and individual faces. While the policy was not announced for several months, Google claimed that they had voluntarily adopted it only 10 days after launching the service.\textsuperscript{135} This twin approach (pre-emptive blurring plus a post-facto allowance for take-down requests) to privacy complaints has now been adopted by all three\textsuperscript{136} of the major North American geo-immersive providers. Each has online resources describing their efforts to protect the privacy of individuals captured on their cameras. Google describes its Street View privacy policy in this way:

Street View only features photographs taken on public property and the imagery is no different from what a person can readily see or capture walking down the street. Imagery of this kind is available in a wide variety of formats for cities all around the world. We are committed to respecting local laws and norms in each country in which we launch Street View. Blurring technology and operational controls like image removal are among the ways in which we ensure that an individual's privacy is respected. We make it easy for users to ask to have photographs of themselves, their children, their cars or their houses completely removed from the product, even where the images have already been blurred.\textsuperscript{137}

Microsoft addresses privacy concerns relating to Bing Street Side privacy as follows:

As with all Microsoft technology, street level imagery and Bing maps were designed with security and privacy concerns in mind. Our mapping products comply with applicable laws governing the acquisition and publishing of imagery. Specifically, we use automated software and advanced algorithms to detect and blur faces and license plates to protect individual privacy. This automated software and advanced algorithms are based on years of Microsoft Research investments in computer vision techniques. We also accept requests to blur or remove images of faces or persons, homes, cars, acts of violence, nudity and unlawful material. We review every request. Depending on the


\textsuperscript{136} Mapquest currently has no privacy policy explicitly related to its mapping service, though its imagery is of a relatively low quality, lessening the need for blurring technologies.

content of the imagery we may remove it entirely, blur a portion of it or take no action if no identifying features remain visible.\textsuperscript{138}

Canpages describes its privacy protections in a similar fashion:

In providing Canpages Street Scene Service, Canpages has been sensitive to avoid including photographic information which would provide personal information about identifiable individuals. We are sensitive to the privacy concerns that might be raised by individuals who were photographed during the preparation of the data required by the Street Scene service. Photographs of identifiable individuals are in no way required by the service. The assembly of the data is designed to deliberately blur the faces of any individual who may be photographed in this process. You will notice as a result that no individual can be identified while using the Mapjack service. If you wish to report a privacy concern, please do so by clicking the “report a concern” on one the Street Scene Service Page.\textsuperscript{139}

The built-in privacy safeguards for these services all follow this twin approach – automated blurring of individual faces and licence plates, along with the option for users to request the deletion of specified images. However, geo-immersive technology-based maps are beginning to increasingly incorporate not only imagery that the commercial providers themselves capture through camera-equipped vehicles, but also images captured and uploaded by users themselves, which are not subject to the same automatic blurring safeguards. Street View, to return to the canonical example, allows any user to upload a photograph of a particular spot to its mapping database, and it then becomes viewable by anyone.\textsuperscript{140} As a user navigates through a particular location in the system, they are able to click on links to those photos of the same area uploaded by other users; Google suggests this functionality is a means of “empowering [its] users.”\textsuperscript{141}

Microsoft’s Bing Maps also features user-generated content, in a fashion that goes even deeper


\textsuperscript{139} “Visitors to our website”, Canpages, online, \url{http://www.canpages.ca/hm/privacy.jsp}, accessed Oct 28, 2010.


\textsuperscript{141} Anguelov et al., supra note 87 at 34.
than Google’s. Their Photosynth service uses powerful algorithmic computing to identify similarities in hundreds or thousands of independently taken images of a particular place, combining them into a single three-dimensional map. Microsoft describes this power as allowing users to “transform [their] regular digital photos into a three-dimensional, 360-degree experience” and that this “constitutes an entirely new visual medium.”¹⁴² But it is not only valuable for individual use – Photosynth can also be used to recreate an explorable version of a particular public space by collecting hundreds or even thousands of independently taken photographs – one of the first demonstrations of its power was combining over 400 user-sourced photos with 200 media-sourced photos of the first Presidential inauguration of Barack Obama into a single explorable version of the scene.¹⁴³ While Photosynth started out as a separate technology group within Microsoft, they are now integrated into the Bing Maps group and Photosynth technology is gradually being incorporated into Bing’s street level mapping system, allowing individually taken images to fill in any gaps in the virtual world that the camera-equipped cars may have missed. This means that commercial efforts at street surveillance of public spaces are likely to be supplemented by user-generated content, which will not be subject to the default privacy protections of the relevant service.

Nonetheless, at the moment the majority of imagery included in geo-immersive projects is of the automatically collected variety, and therefore subject to automated digital blurring of faces and licence plates. However, the blurring approach is not without notable flaws. In a 2009

presentation to the IEEE 12 International Conference on Computer Vision, Google engineers tasked with developing the blurring system outlined four challenges they faced in the project.¹⁴⁴ First, the vast amount of imagery captured by the project required them to develop fully automatic, optimized algorithms, which required significant computer resources. Second, they had to develop an imaging system that could detect the faces of people in a variety of poses and conditions, at different distances from the camera, sometimes facing partially away, sometimes wearing hats or large glasses, sometimes in the shadow, undertaking activities, etc. Third, prior to development of Street View the best automated blurring systems in the world could only successfully pick out faces from a crowd approximately 78% of the time, but Google wanted a near perfect rate. Fourth, they had to limit the false positive rate, then obscure the true positives (actual faces/plates) in a way that rendered them unrecognizable, yet not do so in a manner that was obtrusive to the end user. Google engineers now claim the system used for blurring in Street View achieves an effective blur rate of 89% on faces, 96.5% on US licence plates, and 93.6% on EU plates (no statistics were reported for Canadian licence plates, but there is no reason to assume the numbers would be dramatically different).¹⁴⁵ The other major players have not released data on the accuracy of their blurring efforts, but it is reasonable to assume that they too are striking a success rate of somewhere between 80 and 90%. When one considers the amount of imagery that these systems are generating, if (at best) one in ten faces go unblurred before an image is posted, this suggests that a significant number of individuals will remain identifiable despite Google or Microsoft’s best efforts; Figure 12 is an example of one such image.

¹⁴⁵ Ibid.
More significantly, however, is the reality that even if the effective blur rate does ultimately reach 100%, with no false positives, the possibility of identification of individuals in blurred images would not necessarily be eliminated. As useful as blurring may be, and as impressive as the technology Google’s engineers have developed is, the human brain has powerful ‘processing algorithms’ of its own – individuals can be identified via many means, and the better you know the individual, the easier it is to identify them by reference to blurred facial features, or without reference to facial features at all. We might identify an individual we know by any combination of their manner of dress, their approximate size or shape, their gait, their location – blurring of

---

faces changes none of these things. Indeed, most people would have little trouble recognizing their spouse, immediate family members, or close friends walking down the street facing in entirely the opposite direction – blurring of faces is irrelevant in such a scenario, but the possibility of identification remains.

The real-world usage of Street View and similar geo-immersive systems is already bearing this theory out. In one reported example, for instance, a man was able to identify his wife (despite her face being blurred) in a series of Street View images by reference to the neighbourhood she was walking in and the presence of their dog (See Figure 13).  

![Figure 13 – Woman and dog.](image)

In another example, Google agreed to remove the image of a young woman who had subsequently made news as a murder victim – her family was able to identify the image of her simply by reference to her general shape combined with the location of the image. Even if one eliminates all these extra ‘clues’ upon which identification of an individual can be made and the reference is only to digitally blurred faces (that is, eliminating other information such as location, dress, size, etc.), research shows that humans have a remarkable ability to still accurately determine identity. In one study, subjects were able to recognize the twelve ‘well-known’ faces in Figure 14, despite being heavily blurred, more than half the time – the researchers concluded that “humans can recognize familiar faces in very low-resolution images”, and that “the ability to tolerate degradations [in image quality] increases with familiarity.”

Figure 14: Blurred faces.

---


While currently geo-immersive technologies primarily use vehicles with cameras attached to roam public spaces, it is entirely possible that an expanded systems could use permanent fixed-location cameras (located in private buildings but facing public space) in high traffic areas to provide continual and updated views of a particular locale. Other services already exist allowing the geo-immersive exploration of the interior of private buildings – businesses pay for the privilege of being included in the system (so far this has not implicated any privacy issues, as the photography is done upon request and does not include images of employees or shoppers).\textsuperscript{151} Google is in the midst of rolling out a similar service that will be integrated into Street View.\textsuperscript{152} As more companies enter the geo-immersive technology space, the imaging will likely become more frequent and the pictures of higher quality as those companies compete to provide better products. Google has already shown rapid innovation in how it acquires its imagery, and there is no reason to expect that this process will slow down. Indeed, the team behind Street View has expansive plans for the future:

Looking forward, we will continue to explore new interfaces, find better ways to integrate more user photos, map and photograph places such as malls and museums, and develop platforms to extend coverage to other places where cars cannot go.\textsuperscript{153}

This thesis does not argue, however, that geo-immersive technologies are an irretrievably ‘bad thing’. In general they have largely proven popular and have been accepted by most consumers, and with good reason: there are many positive aspects to the services offered. From tourists wishing to get a sense of the area they will be visiting before they arrive, to prospective homebuyers investigating neighbourhoods on the other side of the country, to individuals

\textsuperscript{153} Anguelov \textit{et al.}, supra note 87 at 37.
nostalgically wishing to revisit the areas in which they grew up, the ability to ‘virtually explore’
public spaces has proven to be attractive for many. Some have attempted to convert Street View
into a stage for performance art,\textsuperscript{154} while others simply choose to devote leisure time to seeking
out amusing or interesting actions caught on by geo-immersive cameras.\textsuperscript{155} The benefits also go
beyond the individual – municipal authorities, for instance, also have a strong interest in having
their cities captured by the process – to be excluded from the list of those captured might
suggest that their city is too small or backwards to be relevant. Indeed, there is already evidence
that communities are \textit{requesting} that they be re-photographed in order to improve their image –
city officials in Windsor, Ontario, complained about the initial capture of images of their city as
they were taken during a municipal garbage strike; Google agreed to re-take images.\textsuperscript{156}

Geo-immersive technologies have also begun to be leveraged in ways not necessarily
anticipated by their developers. Google, for example, allows access to its raw mapping data
through the ‘Google Maps API’, or ‘application programming interface’. The API is a free
service (for non-commercial use) that allows developers to “embed the robust functionality and
everyday usefulness of Google Maps into… websites and applications, and overlay [other] data
on top”\textsuperscript{157}, opening up a surprising number of possibilities. Demonstrating the artistic potential
of the API, Canadian music group Arcade Fire commissioned an online music video that

\begin{footnotesize}
\begin{enumerate}
\item[154]\textsuperscript{154} There are countless examples, but for two see “Street View Performance Art”, online,
Becomes a Stage for Performance Art”, online, http://www.switched.com/2008/11/07/google-street-view-becomes-
\item[155]\textsuperscript{155} See Chapter 4, \textit{infra}.
\item[156]\textsuperscript{156} “Google Street View to Expand in Canada”, CBC News, Mar 22, 2010, online,
\item[157]\textsuperscript{157} The available code includes access to not only the typical mapping interface, but also all available Street View
imagery. Google Maps API Family, see http://code.google.com/apis/maps/index.html and
\end{enumerate}
\end{footnotesize}
combined Google’s mapping imagery with conventionally filmed elements. The hook for the viewer was that it was ‘customizable’ – the initial input asked for the viewer’s childhood address, and the API then incorporated elements from both Google’s satellite imagery and their Street View resources of that address into the music video. The video was a huge success, and helped demonstrate that data and imagery is often used in ways unanticipated by the original collector of that information.158

So, I readily agree that geo-immersive technologies are indeed impressive and can bring with them a host of potential benefits; I by no means seek to eliminate them entirely. However, in the following chapter I want to also argue that, sufficiently widespread, they form an infrastructure of surveillance that, by creating the potential for unanticipated exposure in public places to a mass audience spatially and temporally removed from the original site, may bring about negative social effects – not only for the individuals caught by the unblinking eye, but for society in general. These potential harms, I ultimately argue, demand some kind of legal response to prevent them from arising.

158 The project can be experienced at http://thewildernessdowntown.com, online, accessed Sep 20, 2010.
Chapter 3: Understanding Geo-Immersive Technologies as a Surveillance Practice

In this chapter, I want to argue that geo-immersive technologies ought to be understood as forming the beginnings of a new surveillance practice that, if left unchecked and unregulated, may bring with it the potential for serious social harms. I will canvas the work of surveillance scholars who suggest that the core requirements for defining something as a “surveillance practice” are that it subjects individuals to scrutiny, for the purpose of influencing their behaviour. I will argue that even though geo-immersive technology providers have absolutely no interest in influencing the behaviour of those who may be captured in the imagery, the existence of a secondary surveillance structure composed of unknown numbers of ‘Little Brothers’ – those who view the imagery on their computers – in fact means that the power to influence the behaviour of those observed remains.

Surveillance Theories: Scrutiny for the Purpose of Influence

That surveillance exists for the purposes of influencing the behaviour of the observed is at the heart of surveillance theories in general. According to Lyon, for instance, the “common denominator [of surveillance practices] is that [they place] people or populations under scrutiny... surveillance tries to make visible the identities or behaviour of people”, in order to “influence[e] or manag[e] those whose data have been garnered.” Ericson and Haggerty likewise consider modern surveillance to “involve the collection and analysis of information

---

about populations in order to govern their activities.”¹⁶¹ For Johnson and Wayand, it is “a set of practices that gather and collect data about individuals or entities, with or without their knowledge or consent, for purposes of an analysis which sorts those individuals or entities on the basis of their behaviour or characteristics.”¹⁶² Thus, surveillance can be understood not simply as unfocused observation, but rather “the focused, systematic, and routine attention to personal details for the purposes of influence, management, protection, or direction.”¹⁶³

This also means that surveillance incorporates far more than agents of the state ‘tapping’ the telephones or taking long-distance photos of an individual in order to determine and record their activities. Modern day surveillance also includes the processing of the information ‘flows’ that are generated by individuals as they go about their lives; such surveillance is equally the domain of the state and the corporation. Iran, for example, has installed monitoring equipment that provide it with “one of the world’s most sophisticated mechanisms for controlling and censoring the Internet, allowing it to examine the content of individual online communications on a massive scale.”¹⁶⁴ China’s ‘Golden Shield Project’ (often referred to in the media as ‘the Great Firewall of China’) goes even further, moving beyond traditional forms of censorship to include a “massive, ubiquitous architecture of surveillance” with the ultimate aim of integrating “a gigantic online database with an all-encompassing surveillance network – incorporating speech and face recognition, closed-circuit television, smart cards, credit records, and Internet

¹⁶¹ Ericson & Haggerty, supra note 75 at 3.
¹⁶³ Lyon, supra note 160 at 14.
surveillance technologies.”

State surveillance is, of course, not limited to authoritarian regimes. The same technology is also used in democratic states to provide law enforcement with both the technical ability and the legal power to monitor digital communications.

But surveillance is also commonly associated with the profiling of the consumer by corporate interests; in such cases, it can still be understood as an attempt to influence the behaviour of the observed. Commercial surveillance is a pervasive feature of modern industrial states, where it has become a “general tool used to accomplish any number of institutional goals,” ranging from “control, governance, [or] security, [to] profit [or] entertainment.” Lyon finds that there is a “growing density of surveillance practices in everyday life.”

Closed-circuit television (CCTV) is perhaps the most recognized form of surveillance for commercial purposes; “people watching people is now a fundamental feature of commercial management strategy.” CCTV shares some similarities with the operation of geo-immersive technologies, but there are also notable differences. Both are dependent on the recording of a particular space by means of digital cameras (though CCTV cameras usually record moving images, while geo-immersive

---


166 In Canada, for example, the concept of 'lawful access' encompasses the (judicially authorized) interception of private communications for the purposes of law enforcement. Recent legislative proposals (See for example Bill C-46 (the Investigative Powers for the 21st Century Act, online, [http://www2.parl.gc.ca/content/hoc/Bills/402/Government/C-46/C-46 1/C-46 1.PDF](http://www2.parl.gc.ca/content/hoc/Bills/402/Government/C-46/C-46 1/C-46 1.PDF)) and Bill C-47 (the Technical Assistance for Law Enforcement in the 21st Century Act, online, [http://www2.parl.gc.ca/content/hoc/Bills/402/Government/C-47/C-47 1/C-47 1.PDF](http://www2.parl.gc.ca/content/hoc/Bills/402/Government/C-47/C-47 1/C-47 1.PDF)) have demonstrated an ongoing desire on the part of the government to ensure that state agents retain the ability to conduct these interceptions in the face of rapidly evolving communication technologies.

167 Ericson & Haggerty, supra note 75 at 3.


169 Lyon, supra note 160 at 2.

technologies generally record multiple ‘still’ images). Both are largely premised (though not always, in the case of CCTV) on capturing all activities that occur within the field of view of the camera, rather than being targeted at specific individuals. Both offer the possibility of rendering the activities of individuals visible to others far removed from the location of the camera.

Perhaps the most important similarity between typical CCTV and image capture through geo-immersive technologies is the idea that an individual can be captured in an image by happenstance – the individual need not necessarily be (though in the case of CCTV they can be) targeted due to suspicion of illegal or undesirable behaviour, but is captured simply because they happen to be in the field of view of the camera at a particular moment.

On the other hand, while both are forms of camera-based digital scrutiny, there are clear differences. CCTV is typically characterized by the existence of a relatively fixed infrastructure designed to capture images of individual behaviour, whereas the imaging architecture of geo-immersive surveillance is transient – the cars and other camera-equipped vehicles are constantly on the move. But there is nothing about this transient or fluid infrastructure that means it is not ‘true surveillance’. Another distinguishing factor is that commercially-run CCTV cameras are installed on private property (though they may also record public space near that property). Geo-immersive surveillance occurs, however, entirely on public property. However, this too is not relevant to the definitional claim that image capture through geo-immersive technologies can be understood as a form of ‘surveillance’. Another important difference is that of intent – commercial CCTV cameras are installed with the intent of recording the behaviours of individuals within the field of view of the camera, even if they are not focused on any one
individual in advance. Private CCTV cameras may be installed for varying reasons including crime detection or deterrence, or policing consumption more generally, ensuring that ‘undesirables’ (such as the homeless or groups of teenagers congregating without shopping) are kept out of shopping areas. But regardless of this end purpose, the camera is installed with the intent of capturing human behaviour, whether it is that of the shoppers, the unemployed or the destitute seeking to ‘kill time’ during the day, or criminals. While geo-immersive technologies also expose individuals to visual scrutiny, it lacks similar intent – it exists only to record an image of a location; the presence of individuals is unintentional. No claim is made here that Google or other providers have any kind of plan or intent to shape the behaviour of individuals by photographing them as they go about their daily business. So if geo-immersive technology is not an effort by the service providers to influence the behaviour of individuals they capture in the images through visual scrutiny, could this influence be found through another kind of scrutiny?

Modern forms of commercial surveillance tend to be characterized by not only the visual scrutiny of individuals through CCTV, but also the collection and processing of data generated by daily consumer life. Such information-based surveillance has become a feature of “the mundane, ordinary, taken-for-granted world of getting money from a bank machine, making a phone call, applying for sickness benefits, driving a car, using a credit card, receiving junk mail,

171 Hille Koskela, "The Gaze Without Eyes: Video-Surveillance and the Changing Nature of Urban Space" (2000) 4(2) Progr Hum Geogr 243 at 245. Lyon also argues that such individuals are targeted for monitoring and subsequent exclusion because they are not performing the role of ‘consumer’, and therefore this kind of consumer surveillance “mirrors and reinforces social divisions based on levels of ability to consume.” See Lyon, supra note 2 at 156.
picking up library books, or crossing a border on trips abroad."\textsuperscript{172} Indeed, one might legitimately argue that visual observation now forms only the \textit{minority} of consumer surveillance. Instead, the majority is essentially ‘behind the scenes’ – rather than being obvious to the consumer that it is going on (in the way that CCTV cameras are signposted in order to increase their deterrence potential), data processing occurs in the bowels of powerful computers, out of sight and generally out of mind of the vast majority of consumers. Such attempts to glean valuable information about habits, preferences, and behaviours of customers can be understood as an example of ‘dataveillance’, defined by Clarke as “the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons.”\textsuperscript{173} For Solove, this is “a method of watching not through the eye or camera, but by collecting facts and data.”\textsuperscript{174} Transactional data on items purchased can be collected and combined with other “customer geo-demographic typologies based on residence, and lifestyle codes based on socio-demographic characteristics” in order to “enable the calculation of increasingly sophisticated models of customer behaviour… including the prediction of future wants and needs.”\textsuperscript{175} Sometimes this is anonymous data, but frequently it is readily connected to a specific consumer, through loyalty cards, credit cards, etc. As marketers seek ever more detailed information about a consumer, there is a strong incentive for companies to leverage any information they hold. And yet, this information need not, taken individually, be highly revelatory or personal in some way. It is through the power of algorithmic data mining that the

\footnotesize{\textsuperscript{172} Lyon, \textit{supra} note 2 at 4.  
\textsuperscript{175} Martin Dodge & Rob Kitchin, "The Ethics of Forgetting in an Age of Pervasive Computing", (2005) CASA Working Papers (92) at 5.}
secrets of the data are revealed. As Cohen notes, a collection of many small pieces of
information about an individual is “vastly more than the sum of its parts.” Together, these
parts allow individuals to be profiled and categorized, breaking the individual “into a series of
data flows.” As Gandy describes, “a profile is primarily a list of categories that have been
determined to be relevant to some administrative decision that must be made by an organization
with regard to an individual, a group, or class.” Lyon is also focused on this categorization,
calling it the ‘phenetic fix’; he suggests that the data is captured in order to “place people in new
social classes of income, attributes, habits, preferences, or offences, in order to influence,
manage, or control them.” Karas also believes that such profiling is essentially “an exercise of
power through surveillance.”

And yet there also is no evidence that geo-immersive service providers are categorizing
individuals captured in the images they generate in this fashion, or are developing
comprehensive dossiers about them, or have any interest in influencing people at all. Geo-
immersive service providers make no effort to identify or track individuals using their cameras,
nor provide a system by which an individual can be explicitly searched for by name or image in
their service. While this might change (as Rule notes, “what may strike us today as outlandishly
intrusive or fantastically inappropriate demands for personal information may readily be

at 1398.
177 Sean P Hier, "Probing the Surveillant Assemblage: on the Dialectics of Surveillance Practices as Processes of
Pol'y 1085 at 1099.
179 Lyon, supra note 159 at 3.
180 Karas, supra note 72 at 55.
redefined as basic exchanges in tomorrow’s information society”\textsuperscript{181}, there is no evidence that it is currently the case. There is no suggestion that geo-immersive technology providers have plans for their services that involve the collection of personal data for purposes other than publishing their digital maps. This is a critical factor that separates out geo-immersive technology from more conventional forms of surveillance – \textit{the capture of images of individuals in public is merely an unintended consequence of the primary purpose of geo-immersive technology}, which is to generate a detailed and accurate visual record of a particular space and render it available for exploration online. There is therefore a distinction between the purposes of conventional commercial surveillance, which is designed to track the behaviour of subjects or generate profiles related to that behaviour, and geo-immersive surveillance, in which the revelation of individual behaviour by geo-immersive providers is a only the collateral consequence of a broader information-gathering project.

This ‘collateral’ aspect of geo-immersive technologies poses challenges for the conventional definitions of surveillance that are rooted in concepts of individuals being captured in a systematic or routine manner within a device’s sphere of record for the \textit{specific purpose} of altering that individual’s behaviour. However, it is my contention that the \textit{effects} of surveillance are what matters, whether or not the initial collection of imagery is done with the purpose of effecting behavioural change. In the next section, I want to argue that the influence that is the key characteristic of surveillance theories can be felt even absent a centralized, co-ordinated purpose behind the surveillance, thanks to the bifurcation of the geo-immersive surveillance architecture. In short, there is a \textit{secondary} structure of scrutiny applied to geo-immersive

\textsuperscript{181} Rule, \textit{supra} note 66 at 22.
imagery that exists separately from the initial structure of collection and primary distribution represented by the actions of the commercial service providers.

The Bifurcation of the Surveillance Architecture

Geo-immersive technologies are by no means the first surveillance practice to alter the conventional roles of the watched and the watchers. The democratization of digital imaging technology in the quarter-century since then has offered the increasing potential for a re-balancing of surveillance power – instead of individuals only being the targets of surveillance, they now have the power to turn the lens back on the power-brokers of society, in a process Mann terms ‘sousveillance’. Unlike surveillance, which is characterized by “organizations observing people”, sousveillance “resituates [the] technologies of control on individuals.”

![Figure 15 - Surveillance vs. Sousveillance](image)

Figure 15 – Surveillance vs. Sousveillance.

(Arrows represent direction of surveillant gaze; size of text represents comparative power of the parties)

---

Much of Mann’s early work centred around the idea of wearable computing devices that allow the individual to “take their own sousveillance with them” so that they may “confront surveillance by… surveil[ling] the surveillers directly.”

Considered far-fetched when Mann initially conceived of the idea, ‘wearable computing’ technology is now commercially available at relatively low cost, and virtually every modern mobile phone includes a digital camera capable of taking both still images and video. Mann believes that confronting surveillers in this way “reveal[s] and call[s] into question the asymmetrical nature of surveillance” and “disrupts the power relationship of surveillance.” The focus for Mann then is on relationships that are characterized by power imbalance – he seeks to invert traditional hierarchies of power by changing the direction of the gaze. Examples of this inverted gaze (sousveillance) include:

- Customers photographing shopkeepers;
- Taxi passengers photographing cab drivers;
- Citizens photographing police officers who come to their doors;
- Civilians photographing government officials;
- Residents beaming satellite shots of occupying troops onto the Internet.

The advantages and importance of citizen filming/photographing of public spaces have been well demonstrated, perhaps most notably breaking into the public consciousness in 1991 when George Holiday filmed Los Angeles Police Department officers beating Rodney King after a car chase; based on the video, the four officers were charged with excessive force. While their subsequent acquittals led to several days of race-related rioting in Los Angeles, without the video the charges may never have been brought and important conversations about the state of

---

183 Ibid.
185 Mann, Nolan & Wellman, supra note 182 at 345.
186 Ibid.
race relations and police brutality in the United States may never have occurred. Canada too has seen citizen filming of state agents – the tale of “Officer Bubbles” arose during the G20 protests in Toronto. Protestors filmed a police constable arresting a woman after she blew a soap bubble from a child’s toy that subsequently popped against his jacket. The video was widely circulated, and contributed to the public debate about the nature of police overreaction in the face of street protests.187

While the kind of surveillance associated with geo-immersive technologies shares certain elements with sousveillance (i.e. the watchers are not necessarily in a position of recognized power or authority; recording sometimes occurs in public spaces), important differences remain. Sousveillance – as understood by Mann – is explicitly aimed at disrupting the power relationship between individuals and a bureaucratic organization, whether it is state or corporate. Rather than reversing the gaze towards an organization that typically conducts surveillance on the individual in question in order to disrupt relationships of power, any watching done in the context of geo-immersive surveillance is done by individuals upon other individuals, often without any kind of prior relationship whatsoever (indeed, they may not even live in the same country). The only organizational element that is incorporated is the use of particular commercial services for the initial collection and subsequent primary distribution of digital imagery – distinctly, and unlike in the process of sousveillance, the subsequent view of the images is not directed at that organization itself. The purpose of the watching done by users of geo-immersive technologies is fundamentally different – rather than challenging power

relationships with a bureaucratic organization (be it corporate or state), it is focused on targeting other individuals in order to facilitate public shaming or mockery for perceived social transgressions (see Chapter 4). Unstructured point-to-point surveillance might therefore be described as a process of ‘omniveillance’.\(^{188}\) Rather than the unidirectional gaze that characterizes both (traditional) surveillance and sousveillance, omniveillance is best imagined as a constantly shifting web or network.

![Figure 16 – The Omniveillant Web](arrows represent direction of surveillant gaze; size of text represents comparative power of the parties)

In an omniveillant web, threads (each representing a surveillant gaze) from one node (individual) can extend to any other node, and can appear or disappear unexpectedly, leading to an inability to predict with any certainty when one will in fact be under surveillance from

---

\(^{188}\) I base this term on the work of Groombridge, who argues that the multiple points of surveillance that exist in a modern city have converted it into an ‘omnicon’ (See Nic Groombridge, "Crime Control or Crime Culture TV?" (2002) 1 Surveill Soc 30 at 43. ‘Equiveillance’ might also be suitable term, though Mann has used that term elsewhere to describe a situation in which surveillance and sousveillance processes effectively balance each other out. See Steve Mann, “Equiveillance: The Equilibrium Between Sur-veillance and Sous-veillance”, On the Identity Trail, May 2005, online, [http://wearcam.org/anonequity.htm](http://wearcam.org/anonequity.htm), last accessed Oct 3, 2010.
another node. The surveillance associated with geo-immersive technologies shares similarities with this conception of omniveillance, but there are important differences. In the case of omniveillance, instead of a centralized overseer directing the surveillance, there is a decentralized web of ‘Little Brothers’ watching one another. In the case of geo-immersive surveillance, however, these Little Brothers compose only a secondary element to the overall infrastructure of the surveillance, an element that is organizationally unrelated to the primary element responsible for the collection and initial distribution of the imagery. This is an important distinction between the structure of geo-immersive surveillance and other forms of omniveillance, and is difficult to represent in a two-dimensional figure. The infrastructure of geo-immersive surveillance is best understood as being bifurcated between a commercial entity that collects and is the primary distributor of the imagery, and unorganized, amorphous groups of individuals that are the ‘viewers’ and subsequent ‘redistributors’ of the imagery. It is this secondary component – the vast numbers of anonymous watchers, acting together – that gives geo-immersive surveillance its power to influence behaviour. As I will discuss in the next section, the scrutiny applied by these individuals only really has power when they come together to act in groups, even if those groups are temporary or transient in nature. Regardless, this bifurcated structure explains why the lack of intent on the part of the service providers to profile, categorize, or influence the observed ought not to be seen as determinative to the question of whether geo-immersive surveillance ought to be considered a surveillance practice. However, this bifurcated structure is also the reason why I will argue in Chapter 7 that data protection legislation based upon the fair information principles may in fact be adequate to the
task of controlling geo-immersive surveillance. If the system were purely a “peer to peer” example of omniveillance, then this would not be the case.

The systematic image generation associated with the primary component of geo-immersive surveillance is therefore still relevant to understanding its operation and why it has the potential to cause certain kinds of social harms. For example, while there are other instances of public street photography where the ‘viewers’ and creators of an image share no organizational bond (news photography of public areas, for instance), they lack this systematic, methodical image collection and storage into a public archive searchable by specific address. Even though anonymous audiences can pore over photographs published in newspapers, magazines, or online, the form of the initial image generation and the method by which it can be searched is notably different. Geo-immersive surveillance creates, for commercial purposes, a massive archive of public imagery available at no charge to anyone with an Internet connection, searchable by a pinpoint address or by virtual exploration – even the largest newsgathering agencies in the world do not offer such a system. The scale of the imagery – in size, in quality, in comprehensiveness – generated by the primary surveillance architecture means the secondary architecture has tremendous resources upon which to draw. Together, both these components mean that geo-immersive technologies ought to be understood as having the potential to be a surveillant infrastructure.

**Unleashing the Human Flesh Search Engine**

**The Power to Identify**
Lyon suggests a desire to engage in surveillance can be explained in part by ‘scopophilia’, or ‘the love of looking’. Because the images generated by geo-immersive surveillance must be ‘discovered’ or ‘hunted out’ by exploration rather than merely opening a newspaper, geo-immersive surveillance is a breeding ground for scopophiliacs. Even though this thesis is based on the proposition that geo-immersive surveillance will become deeply problematic only when the use of geo-immersive technologies reaches a certain scale, the potential consequences of this emergent surveillance infrastructure are already beginning to appear. For instance, doxyspotting.com is a website devoted to scouring Google Street View for images of women believed to be sex workers; users at home search for images and then mark them on the doxyspotting website in a competitive fashion. The “frequently asked questions” portion of their website states:

**Why spot prostitutes on Google StreetView?**

Google Maps Street View is the ideal voyeuristic tool. People are voyeuristic in nature – men especially. It is very easy to spot a girl with nice big boobs on Google Street View. Spotting prostitutes may seem a bit more difficult. But if you know what to look for, it actually becomes quite easy. For example you can drop the StreetView Icon pretty much anywhere in Madrid’s Zona Industrial de Villaverde and you will be able to spot a hooker on Google Street View. Doxy Spotting is almost a sport. It is the perfect and insuspicious [sic] way to kill some time at work or if you are bored. But be warned – doxy spotting is highly addictive.

When this scopophilia is combined with the possibility of digital sharing of images and a desire for identification of those in them, the probability of positive identification of any individuals captured in that image is significantly increased; this is another critical element of the secondary surveillance infrastructure, since without identification, the potential for influence over the behaviour of those captured in an image is surely lessened. The possibility of identification,

---


even of obscured individuals, stems from what in China has been termed *renrou sousuo yinqing* – the ‘human flesh search engine’.\(^{191}\) Essentially, the human flesh search engine is the coming together of vast numbers of users to analyse imagery or other information on their home computers in order to spot a particular activity or identify a particular individual; the human flesh search engine is able to process vast amounts of imagery with the accuracy of the human brain but thanks to the distributed nature of the task, with the speed of a computer.

Both state and corporate interests have quickly recognized the power of the ‘human flesh search engine’, and are making efforts to harness it. In the UK, for example, the ‘Internet Eyes’ programme is a commercial service that allows citizens to view live feeds of private CCTV cameras at their computer, and report on any criminal or anti-social behaviour they see.\(^{192}\) In perhaps an example of scopophilia *par excellence*, users (incredibly) pay for this privilege, at a rate of £2/month. In exchange, the users deemed to have reported the most criminal behaviour on an annual basis have the chance to win prizes of up to £1000. In the US, a public-private project (receiving $2 million from the State of Texas) advertises the possibility to Internet users of participating in “virtual stake-outs”, allowing viewers to access 18 live streams of government-run CCTV cameras stationed along the US-Mexico border, in order that they may report any “drug trafficking” or “border crime” they believe they have witnessed.\(^{193}\) The scrutiny of public spaces or images by private citizens may, of course, also have positive effects. ‘Neighbourhood Watch’ programmes, for instance, are premised on this very idea, where


neighbours keep an eye out for each other or each other’s property. ‘Amber Alerts’ similarly harness the human flesh search engine for the protection of abducted children, by asking Internet users to widely share details of the alleged abductor on various social networks. While the phrase ‘human flesh search engine’ was coined in China in response to local events, the dynamic which underlies it is by no means geographically limited, and I am adopting it for use in this thesis – digital communities have globally proved adept at taking isolated snippets of behaviour recorded in digital imagery, sharing them, and then working together in order to discover the identity of a previously anonymous individual. The examples that follow indicate that while omniveillance is typically characterized as people watching people in an unstructured fashion, geo-immersive surveillance is more likely to be characterized by individuals working in groups for the purpose of intensively directing surveillance at one individual or other group. While some of these groups may be pre-existing digital communities, membership in them may nonetheless be transient and temporary – surveillant collectives that spring up and then fade away once the goal is achieved.

There have been a series of instances in which online groups seek to identify individuals in digital photographs that have been distributed widely online. For instance, in 2009 a 14 year old boy uploaded a video of himself torturing cats to the video-sharing website youtube.com, with his face obscured in order that he would not be identifiable. Members of the online community known as ‘4chan’ nonetheless identified him by “piecing together information from other social networking websites including Facebook, MySpace and Digg to come up with a name of
a likely culprit.” Even though the boy’s face was not visible in any of the videos he created involving cats, 4chan members were reportedly able to match details in the background of one video to details of a photo of a bedroom that had been posted to a separate social networking site. Since the latter photo had not been posted anonymously, the identity of the boy was revealed. In 2012, when an anonymous employee of an American fast food outlet photographed himself standing in buckets of lettuce that would be later served to customers, the human flesh search engine again went to work. Despite the photograph revealing the ‘perpetrator’ only from the knees down, members of (again) 4chan were able to successfully identify him by reference to the location and date information automatically embedded in the digital image when it was taken. Several members alerted the restaurant manager and asked him to identify the employee based on the time the photograph was taken and the shoes he was wearing (as revealed in the photograph); the employee was fired.

The human flesh search engine is not always successful, of course. In the immediate aftermath of the bombing of the Boston marathon in 2013, users of the online community ‘Reddit’ attempted to identify potential suspects through combing through the massive amount of imagery that had been generated by the event, thanks to the television cameras present to record the race along with still photographs and video taken by tourists. In doing so, however, they published the photographs of countless innocent individuals with no justification for why they had been targeted for ‘identification’ (other than appearing to carry a backpack or being non-

---


white). After much criticism, management of the website issued an apology for the unjustified accusations levelled at those whose images were circulated, and the user initially responsible for beginning the search quit the community (though being anonymous, could easily have re-joined). This is an example of how even when the operation of the human flesh search engine in identifying individuals may have a noble goal (to catch a criminal), it can quickly spiral out of control. I will return to this idea in Chapter 4, when I consider the potential harms of widespread distribution of imagery and discuss the phenomena of the ‘online disinhibition effect’.

The Viral Spread of Imagery

While the human flesh search engine has not yet seemingly been applied to the task of identifying an individual in the context of geo-immersive imagery (though I believe it is an inevitable occurrence), the mass audience that can compose that engine has begun to assert itself in widespread secondary distribution of that imagery. As I have noted, the geo-immersive service provider organizations are responsible for the primary distribution of the imagery they collect – they make it freely available to anyone with an Internet connection. This is critical, since without this initial distribution, it would not end up the hands of the Little Brothers who compose the human flesh search engine that can scour the images in order to help identify (and as I will argue in Chapter 4, potentially shame) those captured in them. However, that

secondary stage is also responsible for widespread “re-sharing” of those images, along with the generation of archives of those images that are not longer controlled by the initial creator. This secondary distribution can be described as being ‘viral’ in nature. Once a digital image goes viral – that is, once countless perfect digital copies begin to spread across the Internet – eliminating it is a Sisyphean task. While it is true that identifiable individuals captured in an image may be able to submit so-called ‘takedown requests’ directly to geo-immersive service providers, such requests are of limited use for several reasons. First, it is dependent on you being aware that such an image even exists – while you might conceivably regularly check imagery of your immediate neighbourhood to see if you have been captured on camera, this is hardly a realistic proposition for all the potential places you might have been subject to an image. If an image of you appears online in a commercial mapping system and you are not even aware that it exists, the option to submit a takedown request is meaningless. But even if you do happen to discover an image of yourself that you wish to have removed, it may have already virally spread beyond the confines of the geo-immersive provider’s website, rendering any takedown request ineffective.

Such spread is not simply a matter of sharing a link to the originating webpage at Google Maps or other competing service – the actual images generated by geo-immersive technologies can be saved to a user’s computer, and then shared directly or hosted by a third party (as in the case of doxyspotting.com, supra). The effectiveness of a takedown request is eliminated since any such

---

199 A request that an image be deleted. Google, for instance, originally allowed takedown requests for any reason, but as of 2013 the reasons for removal are limited to “inappropriate content” or various kinds of errors. It is no longer clear that an individual could request the removal of a standard Street View image simply because it featured them. See https://maps.google.com/intl/en/help/maps/streetview/privacy.html, last accessed Mar 12, 2013.
process, being non-judicial, would only apply to that originating website. While geo-immersive service providers have a copyright interest in the map images they create and typically note that redistribution without permission is a violation of their mapping terms of use, they have thus far shown no interest in pursuing copyright claims against those who host copies of their images.200

As a result, particularly if an image features a compelling, embarrassing, or otherwise notable image, it tends to rapidly go *viral*. The potential for viral spread means that once information (regardless of whether it is in textual or visual form) about us appears online, “we may be famous or infamous in a matter of seconds”201, and there is very little that can be done about it once an image reaches the ‘viral stage’.

Strahilevitz offers an account of such viral propagation, explaining how the rise of online social networks has fundamentally altered the kind of calculations individuals must make before sharing something with even a limited group in an online setting.202 While his theory is not specific to the transmission and re-transmission of images, it is nonetheless instructive. Strahilevitz notes that offline social networks tend to have a large number of poorly connected nodes and a smaller number of highly connected nodes (‘supernodes’). When social groups are closely knit, he argues, information transmission from other groups is less likely, because individuals within the group tend to be similar (the ‘echo chamber’ effect); individuals in closely-knit groups tend to have many strong ties with one another. But supernodes can form a bridging function between closely-knit groups – “the prevalence of supernodes who are weakly


201 Anne Cheung, "Rethinking Public Privacy in the Internet Era: A Study of Virtual Persecution by the Internet Crowd" (2009) 2 J Media L 191 at 192.

tied to multiple different close-knit communities will play a substantial role in determining how quickly and completely new information is disseminated through a society.”

Essentially, the more supernodes there are, the more likely information will be transmitted from one group to another. Strahilevitz suggests that there is a tendency in all social networks for information to be degraded as it passes through the network – only a certain percentage of information will be transmitted. As a result, in the off-line world, a reasonable rule of thumb is that oral information is unlikely to be transmitted beyond two links; individuals can generally have a reasonable expectation of privacy that gossip, for example, will generally not be transmitted more than one stage beyond the close-knit group with which it was shared. But this calculation does not apply to the online world, he says, which has “facilitated the more rapid dissemination of new information and created new categories of supernodes.”

Digital communities (not simply behemoth online social networks like ‘Facebook’, but also ‘message boards’ or ‘forums’ such as 4chan and Reddit) may be more loosely knit than their offline counterparts, because forming an online connection may require less effort than the formation of a friendship in the ‘real world’. Thus, while individuals may have a close friend network in the ‘real world’ of 10 to 20 people, they may have an online network in the hundreds, which may include family, colleagues, offline friends, friends of those offline friends, former lovers, friends of former lovers, fellow students, people they met once at a party, and even people whom they simply exchange messages with regularly on topics of mutual interest, though they have never met personally. Given the prolific spread of online social networks and

203 Ibid.
204 Ibid.
205 Ibid.
other kinds of digital communities, almost anyone can function as a supernode at the click of a button. This means that digital image sharing online is an inherently ‘leaky’ process: using Strahilevitz’s social networks theory, we can expect that the information will be rapidly disseminated from one close-knit group to another, even though those two groups may be weakly connected. Once the image is placed online for sharing even with a limited number of individuals, “disclosure to a supernode will not only increase the number of people who will be exposed to the information at issue, [but] it will also enhance the likelihood that the information will jump across a structural hole” that otherwise separates distinct social groups.\footnote{206} As a result, it is extremely difficult for individuals to control the distribution of images once they are digitized and are able to be viewed by (even a limited) number of individuals beyond the creator/subject. Once an image leaves the hands of the creator, it is effectively impossible to ‘retrieve’ – endless perfect copies of the initial image can be made and transmitted globally at effectively zero cost. Therefore, even though purveyors of geo-immersive technologies may offer the possibility of deleting an offensive image their services capture, it is unlikely to be effective. Once released, the digital genie cannot be stuffed back into the bottle. Google, for instance, makes billions of images available through its Street View service to absolutely anyone in the world with an Internet connection – no membership or registration is required to view them. Any one with basic computer skills can copy ‘interesting’ images from the Street View service to their own machine, and from there the image can virally spread regardless of Google’s intentions or desires. This applies, \textit{mutatis mutandis}, to all geo-immersive service providers.

\footnote{206} \textit{Ibid.}
Once a commercial street surveillance provider publishes the initial imagery to the open Internet, the potential for viral propagation of any image is present. I suggest that while geo-immersive surveillance itself does not constitute an online social network as typically understood (unlike Facebook, or Google+), Strahilevitz’s description of how information spreads is nonetheless applicable to the way in which geo-immersive imagery is shared – the imagery is the content, the social network is the fluid and amorphous groupings that come together to share and redistribute that imagery. Indeed, evidence is accumulating that viral dissemination of certain images from Street View and similar services is already happening, whereby ‘Little Brothers’ take images of note from Street View or similar services, catalogue them so that they can be found easily by others, and thus they then spread virally from one digital community to another. I have already touched on the phenomena of “doxyspotting”, which is a very specific collection of images, though there are various websites devoted to cataloguing and sharing all manner of ‘unusual’ or ‘interesting’ geo-immersive imagery that has been copied from the website of a mapping service provider.

As a brief example, Figure 17 is an image of a Dutch man caught on the Google Street View system urinating by the side of a road. While the original image was subject to a successful takedown request and is no longer available on Google Street View itself, it (and many other similar images) is still available on the websites that catalogue such images.

---

But the viral aspect of the transmission means the images are not even limited to these cataloguing websites – indeed, many of the images I have collected for use in this thesis were taken not from Google Street View or secondary cataloguing websites, but rather tertiary websites such as online newspapers or blogs with relatively few readers, thanks to this process of ‘viral spread’. A quick Google search (of course!) was all that was necessary to start wading through archives of all kinds of surprising imagery which had long since been deleted by Google from the Street View website itself. So this re-distribution or viral propagation of images is part of the secondary surveillance infrastructure that stands apart from the initial collection mechanism. When these kinds of images go ‘viral’ and are widely distributed, the

---

potential for individuals to be identified is greatly increased, thanks to the power of the human flesh search engine.

**Summary**

My argument in this chapter has been that, yes, geo-immersive technologies do subject individuals to the kind of scrutiny we can class as surveillance, though it is not the same as typical commercial data-based scrutiny or the sort visual scrutiny afforded by CCTV, thanks to its bifurcated structure. Unlike many typical forms of visual surveillance, then, any behavioural influence upon or impact felt by individuals unintentionally caught by the cameras therefore stems not from those conducting the initial observation/recording (the commercial entities operating the cameras), but rather third parties (‘the watchers’), associated with neither the subject captured nor the entity doing the capturing. The visual scrutiny associated with geo-immersive technologies is accomplished entirely by third parties, unrelated to either the individual recorded or the organization doing the initial image collection and distribution. It is true that the collection of imagery associated with geo-immersive technologies is not done with the intent of either recording or altering the behaviour of those who happen to be caught in the images. However, I have suggested that the potential for viral spread of the imagery results in a greatly expanded potential audience of ‘watchers’, and the possibility of intense subsequent examination of that imagery means that, taken as a whole, the widespread use of geo-immersive technologies ought to be considered a surveillance practice.

In the chapter that follows, I will argue that thanks to this structure, a widespread system of geo-immersive surveillance would significantly increase the possibility that individuals caught in the
imagery will be sanctioned for any apparent breach of a social norm revealed in that image.

What is more, in the context of ‘online sanctioning’ it is likely to occur in a manner disproportionate to any alleged transgressive activity that is captured. This is, in effect, an attempt by those sanctioners to influence the behaviour of individuals captured in a digital image, but also those in society more broadly, who may be deterred from certain behaviours – even fully legal ones – out of fear of the consequences if they are exposed to a massive, anonymous audience while undertaking those behaviours in public.
Chapter 4: The Potential Harms of Widespread Geo-Immersive Surveillance

In the last chapter I argued that the widespread use of geo-immersive technologies ought to be seen as a form of surveillance that places individuals under scrutiny. In this chapter, I wish to consider in more detail the effects of this kind of scrutiny. I suggest that it may lead to large anonymous groups attempting to identify and subsequently sanction (often disproportionately severely) individuals captured in geo-immersive imagery for perceived social norm violations. I also suggest that ultimately the effects of this are likely to be felt beyond only those who are photographed. While there is not yet evidence that this latter effect is occurring, I argue that this is only because the deployment of the relevant technologies is in its infancy. I suggest that as the infrastructure becomes more widespread, and as ‘shaming’ occurs with greater frequency, individuals will begin to modify their behaviour in order to conform to what they see as the dominant social norms. This in turn may lead to the widespread internalization of socially dominant norms on an unconscious level, as the panoptic effects associated with surveillance occur.

Digital Shaming for the Violation of Real-World Norms

Social norms are typically thought of as “social construct[s] that help describe and explain human behaviour”\(^209\) or tools that help us explain “social regularities that impose informal standards and constraints on human behaviour in deference to the preferences of others.”\(^210\) For

---


\(^{210}\) April M Major, "Norm Origin and Development in Cyberspace" (2000) 78 Wash U LQ 59 at 61.
the purposes of this thesis, when referring to social norms I am considering them as “includ[ing] general, societal expectations for our behaviour, the expectations of valued others for our behaviour, our own expectations for our behaviour, and standards that develop out of our observation of others behaviour.”

Norms “guide and/or constrain social behaviour without the force of laws”, or, as Major puts it, while “laws can and do attempt to reinforce favourable normative behaviour, norms in their purest form are not driven by legal obligations.” Thus, norms “may be independent of laws or they may overlap”, but they do not necessarily require government for “either promulgation or enforcement.” Social norms are, therefore, “patterns of behaviour that are widely adhered to by some group of individuals, at least in part because of social pressures to conform to that norm.” Enforcement of the rule comes from social pressures, generated through a “pattern of informal sanctions.”

For instance, they may be shunned, rebuked, have their social status reduced, face punitive action against their person or property, or be shamed. Whatever the form, social sanctions “can serve as a cheap and pervasive means of deterring… stigmatized behaviour.” Differing forms of sanctioning behaviour naturally often overlap – for instance, an individual may be rebuked and

---

211 Cialdini & Trost, supra note 209 at 152.
212 Ibid.
213 Major, supra note 210 at 64.
220 Miller, supra note 218 at 903.
222 Geisinger, supra note 216 at 612.
publicly shamed, resulting in the lowering of their social standing. Consequently, individuals may feel an obligation to follow norms “because of an internalized sense of duty, or because of a fear of a non-legal sanction, or both.”

The imposition of sanctions on norm-violators also serves to reinforce the strength of the norm among others, as individuals recognize that “violations of the behavioural standard will be punished”, and therefore consciously choose to follow the norm. Sanctioning may be done both by parties who are directly affected by the conduct of the norm violator, and by third parties who are merely aware of the violation but otherwise unaffected by it. It is these third-party sanctions that “greatly enhance the scope for norms that regulate human behaviour”, and they are the force that drives the impact of the secondary level of geo-immersive surveillance vis-à-vis social norms. In this section, I consider cases in which members of digital communities seek not only to identify a perceived norm violator captured in an image, but also to subsequently sanction them. I will suggest that the ‘online’ nature of the sanctioning can easily spiral out of control, leading to calls for punitive actions that appear disproportionate to the alleged violation of the norm. It is my contention that this pattern of third-party online sanctioning is likely to arise in the context of increased deployment of geo-immersive technologies and the consequent scrutiny of vastly increased numbers of individuals captured in the digital imagery. As the number of images generated by geo-immersive technologies increases, so too will the number of instances where a third party – a Little Brother – seeks to enforce a social norm they believe an individual spotted in an image has violated.

223 McAdams, supra note 219 at 340.
224 Ernst Fehr & Urs Fischbacher, "Third-Party Punishment and Social Norms" (2004) 25 Evol Hum Behav 63 at 64.
225 Ibid.
Despite the potential for socially positive experiences with the mass scrutiny of digital images or public spaces, the reality is that the campaigns led by the human flesh search engine tend to be rather more negative, resulting in not only damage to the online reputation of the individuals involved, but in some cases psychological trauma, real world harassment, and even physical assault. A ‘vigilante’ mentality sometimes arises in online communities in response to perceived social transgressions captured in a digital image. This can begin first with a call for identification of the individual concerned, but it frequently also involves a call for the individual to be shamed in some way; Cheung notes that “this last step easily escalates into a form of Internet witch hunting online, mob trial, or harassment in real life.”

The following examples are incidents in which a transgressive behaviour in public was recorded digitally, shared widely online thanks to it spreading virally, and then the subject of online campaigns to either identify and punish the ‘perpetrators’. As will become clear, the level of shaming or sanctioning often goes far beyond what appears justifiable. While I refer to these sanctioning activities under the rubric of ‘online sanctions’, I use the ‘online’ moniker only in reference to the digital spaces in which the sanctioning campaigns are conceived. The activity that led to the sanction need not necessarily have occurred ‘online’, nor are the sanctions only limited to actions taken against the alleged transgressor’s ‘digital life’.

**Dog Poop Girl**

In 2005, a young woman in Seoul allowed her dog to defecate on the floor of a subway car. When other passengers requested that she clean up the mess, the woman declined to do so and

---

226 Cheung, supra note 201 at 193.
reportedly became belligerent. Another passenger decided to take a picture (with her mobile phone’s camera) of the woman and the dog, and posted it to a popular Korean website along with a description of the circumstances. Within days, users on the Internet had determined the identity of the woman, posted personal details of her life online, and began to seek out yet more information about both the woman and her family. Humiliated by the exposure, the woman allegedly dropped out of university in response to the stress, and threatened to commit suicide if the Internet harassment didn’t stop.  

*Bus Uncle*

In early 2006, a passenger on a public bus in Hong Kong asked Roger Chan, who was talking loudly on his mobile phone, to lower his voice. Chan proceeded to berate the younger passenger for six minutes for daring to question the manner in which he talked on his phone. The incident was captured on the video camera of a third passenger’s mobile phone, and uploaded to a website. While Chan initially became a minor celebrity and seemingly enjoyed the exposure (the video was ‘remixed’ into a karaoke song), he soon became a victim of the video’s notoriety, and was harassed for his actions on the bus. Two weeks after the video was released, three men assaulted Chan in his workplace, apparently in response to the video. 

---

**Cat Bin Lady**

In August 2010, a private CCTV camera installed at the front of a suburban English house captured a video record of a woman walking by, nonchalantly picking up a cat, and then throwing it into the nearest rubbish bin. After the owners of the cat (and the CCTV camera) discovered it unharmed inside the bin, they uploaded the footage to a video-sharing website in order to determine the identity of the perpetrator. The video rapidly spread virally and users of 4chan launched a campaign to discover the woman’s identity, ultimately successfully identifying her as 45 year-old Mary Bale.\(^{231}\) Anonymous Internet users then proceeded to post this information online, along with her phone number, a Google Street View image of her house, her place of employment, and the phone number of her supervisor at her place of employment, who also received harassing phone calls. Bale went into hiding and required temporary protection from the police, who stated they were concerned about “the level of vitriol” Bale was receiving.\(^{232}\)

**Puppy-Throwing Girl**

In September 2010, a video emerged online showing an unidentified girl throwing puppies into a river in order to drown them. Outraged, users of online forums (again, primarily but not exclusively 4chan) shared as much information as they could glean from the video in order to track down the girl, exhorting each other to “find this dumb bitch and throw her in a river” and


“steriliz[e] and impriso[n]” her, with some even stating that she ought to “die in a fire.” After discovering the location of the individual who had uploaded the video, the girl was eventually identified as Katja Puschnik, a 12-year-old Bosnian. Puschnik, her family, and friends were all subject to harassment both online and off, ultimately leading to police involvement. While she originally faced animal cruelty charges, it was later revealed she was too young under Bosnian law to be charged, leading one website to conclude that even though she would not face punishment by the state, her “online life [would be] screwed for a long time.” While it is impossible to predict the accuracy of that conclusion, it is interesting to note how reputation online can be thought of as equally important as (and fundamentally connected to) one’s reputation in the ‘real’ world.

This suggests that not insignificant reputational harms can befall an individual as a result of being captured in a digital image. But is having our reputation destroyed by one thoughtless act a justifiable punishment, even for an admitted transgression? If harm to our reputation is essentially harm to our “ability to engage in basic activities in society… [because] we depend upon others to engage in transactions with us, to employ us, to befriend us, and to listen to us,” then having the proper legal tools to protect that reputation is vital. As Solove questions,  

---

237 Solove, supra note 174 at 31.
why “should people’s social transgressions follow them on a digital rap sheet that can never be expunged?”\(^{238}\) However, other than ensuring that there is some proportionality in the consequences, I am not particularly concerned that the activities of the ‘Puppy Throwing Girls’ of the world may come to light; the revelation of truly abhorrent public behaviour is probably a net benefit. I am more deeply concerned about what the kind of mass campaigning against the Puppy Throwing Girl represents to other people in society, and its potential for application in rather more innocuous scenarios than killing dogs. Consider the example of Ghylsain Rasa, also known as the ‘Star Wars Kid’; while unrelated to the use of geo-immersive technologies, his story is nonetheless an instructive example of the effects the viral transmission of digital imagery can have.

In 2002 Ghylsain, then a high school student in Trois-Rivieres, Quebec, filmed himself swinging a golf club in an attempt to recreate scenes from the well-known fantasy movie ‘Star Wars’, in which the characters duel with sword-like ‘light sabres’. The videotape was discovered by a fellow student, and at some point was uploaded onto the Internet. By 2006, thanks to its viral transmission online, the video had been viewed over 900 million times.\(^{239}\) Widely mocked online by the viewers of the video, Rasa dropped out of school, was diagnosed with depression, and eventually ended up in a children’s psychiatric ward.\(^{240}\) Rasa and his parents commenced a lawsuit against the three students who had found, digitized, and initially

\(^{238}\) Ibid.


uploaded the video to the Internet, claiming that he “had to endure, and still endures today, harassment and derision from his high-school mates and the public at large.” The lawsuit was settled in 2006 for an undisclosed sum, and, on a happier note, Rasa went on to successfully complete law school at McGill University.

While Rasa’s story finished on an upbeat note, this is not always the case. I have already discussed the campaign by users on Reddit to hunt down and identify suspects of the April 2013 bombings of the Boston Marathon by scouring through available imagery. But their amateur sleuthing was not limited to looking at photographs – they also listened in to police scanners through websites that record and make the audio streams available to anyone in the world. One anonymous user believed he or she had overheard the police naming a particular individual as a suspect, and they shared this information with the rest of the Reddit group. From there, the information virally spread across online social networks of all kinds, just as Strahilevitz’s theory would predict. Sunil Trapathi, a 22 year old philosophy student attending Brown University, had been missing from home for the past month; this, concluded the users of Reddit, Facebook, and other networks, was surely an indication of his guilt – he must have been away from home planning the attacks. Users bombarded his family with hate mail, media trucks camped outside his parents’ home, and his Facebook page was defaced. On April 25, several days after the

241 Ibid
243 Of note, it took a full six months from the date of the creation of the original video in the Star Wars Kid case (via an old VHS-tape based home video camera) to its digitization and uploading online. Furthermore, the initial spread of the video online pre-dated the advent of video-sharing websites such as youtube.com, and yet ‘viral spread’ was still achieved. The technology has already changed from Rasa’s time to eliminate that kind of time delay: videos can be instantly uploaded directly from one’s mobile phone to video-sharing services – separate video cameras and computers have quickly been rendered unnecessary, making rapid viral transmission all the more easy.
actual suspects had been identified and captured or killed, Traphathi was found dead, an apparent suicide. While at the time of writing there is no evidence that Traphathi killed himself as a direct result of the accusations that he was a terrorist, there is certainly evidence that his family was subject to significant harassment thanks to the viral propagation of a single misheard name.

These examples serve to show the power that the viral propagation of information, particularly imagery, can have. I am ultimately less interested, however, in the damage to individual reputation that may result from the use of geo-immersive technologies, and more interested in the broader adoption or internalization of certain social norms to which they may lead – even though that adoption may be driven in part by a desire on the part of individuals to avoid reputational risks. While I will return to this argument in greater detail later in this chapter, it is necessary to first consider explanations for why online communities seek to sanction those they feel to have violated some particular norm, and why there appears to be such a disconnect between the nature of some of the alleged infringements and the sanctions for which are called.

Why Do Online Communities Seek to Enforce Norms Against Others?

In many of the examples above, individuals or groups attempted to sanction the behaviour of individuals they had never met for an action that could not have personally harmed them. Why? Miller suggests there are at least four different reasons why individuals enforce norms. The first is to stop or deter conduct that they find offensive or harmful to themselves on a personal

---


245 Miller, supra note 218 at 906.
level. The second is the ‘esteem gain’ theory proposed by McAdams, which suggests that individuals may follow norms not only to ensure they do not lose respect, but that they will also seek to enforce norms as a means of receiving the esteem of others. McAdams contends that social norms arise when sufficient numbers of individuals punish behavioural transgressions by withholding from the violators esteem, or ‘the good opinion or respect of others.’\textsuperscript{246} McAdams believes that

\begin{quote}
[\textit{I}f individuals desire esteem… it necessarily follows that one who violates a consensus incurs a cost. The esteem cost is the probability that a violation of the consensus will be detected, multiplied by the value of the esteem that would then be lost. A norm arises when, for most individuals in the population, this esteem cost exceeds the cost of following the consensus.\textsuperscript{247}
\end{quote}

Under this theory, individuals seek to enforce norms as a secondary method of gaining esteem; that is, esteem is gained not only by following norms, but policing the behaviour of others. The third reason, according to Miller, is Eric Posner’s ‘signalling’ theory, which argues that third parties enforce norms against others as way of signalling their trustworthiness to future partners. Posner argues that people follow norms not because of concern for esteem, but “because they are engaged in a signalling game in which people engage in behavioural regularities in order to show that they are desirable partners in cooperative endeavours.”\textsuperscript{248} For Posner, there are two ways in which signalling can result in the behavioural regularities that become social norms. First, individuals may engage in costly actions such as shunning or rejecting norm-violators to signal that they are trustworthy (unlike the norm-violators), and value future co-operation. Second, individuals may engage in lower-cost actions such as conforming to the norm to avoid punishment by individuals signalling their own type through the costly actions of shunning or

\begin{footnotes}
\textsuperscript{246} McAdams, \textit{supra} note 219 at 355.
\textsuperscript{247} \textit{Ibid}.
\textsuperscript{248} Posner, \textit{supra} note 217 at 5.
\end{footnotes}
The fourth reason for enforcing norms against others, according to Miller, derives from a simple sense of internal satisfaction in enforcing norms, even when the violation in no way impacted the enforcer personally. Rather than seeking out the esteem granted by others, as in the McAdams model, then, this concept is focused purely on an internal sense of well being when either following or enforcing norms.

Miller believes the four reasons will fluctuate depending on whether the situation is best described as a co-operative or non-cooperative setting. Co-operative settings are “those contexts where people interact with one another frequently over an extended period of time”, while non-cooperative settings are “those in which the interacting parties are strangers who do not expect to deal with one another again.” Miller believes that signalling and esteem theories are less likely to be operative in non-cooperative setting (such as in the case of the tipper in a foreign land), and therefore if we can see norm enforcement in non-cooperative settings it must be because “people believe the norm to be valuable in itself.”

Is this in fact the case with the kind of sanctioning associated with the human flesh search engine? Interestingly, the setting of such sanctioning appears to fall somewhere in between Miller’s co-operative and non-cooperative definitions. The bifurcated nature of the scrutiny associated with geo-immersive technologies also applies to most examples of the way the human flesh search engine has thus far been seen to operate – digital communities like 4chan (in the immediate examples above) or Reddit (in the case of the Boston bombings) derive their power from the ability to scrutinize images that have been spread virally, rather than imagery they have

\[249\] Ibid.  
\[250\] Miller, supra note 218 at 899.  
\[251\] Ibid.
personally generated. As a result, the participants in the scrutiny and any subsequent shaming exist in a realm that shares elements of both co-operative and non-cooperative, as understood by Miller.

On the one hand, groups have undertaken all the scrutiny I have discussed above. While the individuals that make up those groups may be dispersed and in effect ‘working alone’, their efforts are collaborative – in each of the examples, a centralized page on 4chan or Reddit was used to host all new information about the subject being searched for or shamed, in order to avoid members duplicating efforts. The fact that these are digital communities does not eliminate the ‘community’ aspect – people often feel emotionally invested in their online personas, and have meaningful and regular interactions with those they come across online. In such cases, online shaming appears to fit relatively well with Miller’s conception of a co-operative setting, and it therefore may be the case that it is more likely that individuals within those communities are competing for esteem or signalling trustworthiness. However, there are two possible objections to raise here. First, online sanctioning associated is typically done anonymously. If users are anonymous, then it is not a co-operative environment in the way Miller envisions, because the anonymity destroys any possible future use of an existing relationship, unless users maintain pseudonyms over an extended period of time and become ‘known’ by them. The second possible objection here is that anyone can join these

---

253 In certain cases, ‘anonymously’ may not mean simply in the sense of individuals using a pseudonym, but also in the sense that *all* postings in the community are attributed to “anonymous” (hence the moniker of well-known hacker group “Anonymous”, which originated out of the /b/ sub-board of the 4chan community). In such instances, the members could not be competing for esteem, because there is often no way of knowing ‘who is who’, due to the lack of pseudonyms.
communities, if they are motivated enough. In such contexts, many of the individuals involved may have absolutely no connection to one another, springing up temporarily when motivated by a particular transgression, never to be heard from again. In this sense, they may form a temporary or transient digital community, devoted to a particular task, but the lack of permanence means the necessity to send positive signals to other group members through enforcement of norms is not present. Indeed, while (comparatively) close-knit digital communities tend to be the initial site of social sanctioning in the context of the human flesh search engine, thanks to the viral spread of information the process can often spreads to broader social networks and then the offline community (as in the case of the hunt for the Boston bombers, Bus Uncle, and others). Thus, the process of social sanctioning online also shares elements with what Miller described as non-co-operative settings, in which they seek to enforce norms largely out of personal offence they perceive as a result of the norm violation, rather than in order to gain esteem from others within the group or in order to signal trustworthiness.

Interestingly, Miller also predicts that the form sanctions will take will differ depending on whether or not the setting is co-operative or non-co-operative. In non-co-operative settings, Miller believes that only immediate sanctions are available – those that can be enforced against the violator at the moment of transgression, including “personal rebuke or punitive action against person or property, or oblique rebuke, by offering friendly advice, irony, sarcasm, nonverbal cues, etc.”254 In co-operative settings, however, he suggests that there is also the potential for long-term sanctions, administered after the transgression and that may also be carried out by third parties; examples include “damag[ing] the violator’s reputation by gossiping

254 Miller, supra note 218 at 903.
or badmouthing… shunning or stigmatizing.” Miller argues that in non-cooperative settings, such sanctions are meaningless because there is no point in shunning or shaming someone you will never see again. Sanctions imposed by online communities, whether they are of the more permanent or transient variety, pose challenges to this framework. For instance, the form of sanction is often rebuke and punitive action against the violator. Such sanctions are typically understood by Miller to be ‘immediate’, but in the context of online sanctioning it is always ex post facto to the violation. At the same time, the vast majority of online sanctions appear to be done by third parties with the goal at least in part being damage to the reputation of the violator. Miller would understand these as long-term sanctions, even though there is little probability of the Little Brothers meeting the subjects of the campaigns in ‘real life’ once the campaign is over. Admittedly, such sanctions may lead to individuals who do in fact know the subjects in ‘real life’ becoming aware of their alleged transgressions, and thus the possibility for effective ‘shunning’ may still exist.

In general, the kinds of social sanctions associated with online shaming stemming from the scrutiny of digital imagery generated by geo-immersive technologies are likely to differ from those we may have traditionally expected in the offline context. The scopophilia that drives the desire to look is combined with either a desire to punish transgressors who are seen to violate a particular social norm (in the context of both transient and more permanent digital communities), or a desire to signal positive in-group behaviour (only in the context of more permanent digital communities). In my view, the difference in ‘real world’ sanctions and

---

255 Ibid.
256 Ibid.
sanctions driven primarily online lies in the fact that they tend to be inflicted primarily by third parties, lacking any connection to the violator at the moment of the transgression. These third parties seek to impose punitive sanctions and shame violators, but in a manner far more severe than might typically be the case in the offline context. In the next section, I describe the reason why such sanctions that grow out of online communities, be they transient or more permanent, can quickly spiral out of control.

The Online Disinhibition Effect

Social norms, conformity to them, and sanctioning behaviour for their violation are all natural, and indeed necessary, parts of society – we may feel pressure to conform at home, in the workplace, on the street, through media, through the state, etc. It is not that all conformity to social norms is inherently a negative process – each and every one of us conforms to a greater or lesser extent to a consensus that helps lubricate society, whether it be as simple as standing or walking on a particular side of an escalator or as nuanced as the many (and varying) rituals that accompany a dinner with a distant family member, a professional colleague, or an intimate partner. What, then, is it about sanctioning online that is particularly concerning? I have indicated that geo-immersive surveillance adds a new and different dimension to the transmission and enforcement of social norms that should not go unnoticed – it transforms the viewing audience (those who might witness an activity that runs contrary to a majority norm) from those immediately present at the site of the activity, spatially and temporally, to a global audience of billions, stretching into the future for all time, thanks to the permanence of the digital record. In this section I want to suggest that this change in the viewing audience to one composed largely of anonymous commentators in unknown locations means that the sanctions
used for norm enforcement may frequently be disproportionate to the nature of the alleged offence. While this does not necessarily mean that a different set of norms is being enforced, it does mean that the social pressure we may feel from geo-immersive surveillance is likely to be very different than the social pressure we may typically feel in other situations. While scopophilia might explain the desire of individuals to browse through images they find online, it does not explain the vitriol that can be whipped up by transgressions captured in those images, even when they are relatively minor.

The gap between the alleged infraction and the punishment doled out by the anonymous crowd can be vast; online shaming “targets people without careful consideration of all the facts and punishes them for their supposed infractions without proportionality.”257 There is thus an apparent disconnect between how individuals act online and how they act in the physical world when it comes to shaming or sanctioning others for perceived norm violations. This disconnect has been described in the psychology literature as the ‘online disinhibition effect’.258 Suler contends that there are six inter-related factors that contribute to this effect; he suggests that while some individuals experience the effect in only the presence of one or two of the factors, when multiple factors are present the effect is amplified.259 The first of these he terms ‘dissociative anonymity’. Suler suggests that online, most individuals can hide their identity, and to the extent that they “have the opportunity to separate their actions online from their in-person lifestyle and identity, they feel less vulnerable about self-disclosing and acting out… in

---

257 Solove, supra note 174 at 102.
259 Ibid.
the case of expressed hostilities, the person can avert responsibility for those behaviours."260

The second factor is ‘invisibility’ – in the online world people are essentially invisible, “giving people the courage to go places and do things they otherwise would not.”261 While this certainly has beneficial aspects in terms of individual freedom, mutual invisibility to one another eliminates the ability to read body language, and so also means that individuals online “cannot see any disapproval or indifference that might inhibit what they are going to say”.262

Suler describes the third factor as ‘asynchronicity’, meaning that interaction online is rarely done in ‘real time’. He suggests that while in real life we have to cope with immediate reactions for our behaviour, inhibiting us to some extent, online “people’s train of thought may progress more steadily and quickly towards deeper expressions of benign and toxic disinhibition.”263 The fourth factor Suler terms ‘solipsistic introjection’. He suggests that the lack of face-to-face cues in the online world means that individuals tend to ‘shape’ the personalities of those with whom they are interacting by filling in the gaps with elements of the personalities of other people they know, or of celebrities, or of themselves. He contends that conversations [conducted] in this way may be experienced as an almost internal dialogue with oneself, “unleashing many powerful psychological issues.”264 The fifth factor is ‘dissociative imagination’. This is connected to the aforementioned introjection, whereby since we imagine people online to be a certain kind of person regardless of the kind of person they actually are, it becomes easier for us to disassociate “online fiction from offline fact, leading some to see the online world as a kind

260 Ibid.
261 Ibid.
262 Ibid.
263 Ibid.
264 Ibid.
of game with rules and norms that do not apply to everyday living.” Finally, Suler suggests that interactions online are characterized by “the minimization of status and authority”; this is a reflection, he contends, of the traditional Internet atmosphere of apparent equality and a lack of centralized control, which tends to lower inhibitions. Suler notes that all these six factors will vary in their intensity and effect given individual differences and predispositions, but together they help to explain the disconnect between behaviour online and off.

The online disinhibition effect can manifest itself in benign ways – people willingly sharing personal details about themselves online with strangers, for instance. In terms of information sharing, Kane contends that there is an important psychological element at play, suggesting that social networks are characterized by a “sense of connecting coupled with a fear of being left behind”, creating pressure to continually share more and more about their lives. He believes the “intensity of this pressure cannot be discounted”, and goes some distance in explaining the immense popularity of online social networks. Youth are particularly vulnerable, Kane argues, to both pressure to accumulate a large number of online ‘friends’ and to regularly share personal content with them, meaning their personal privacy is “often willingly and easily sacrificed.” Gelman believes the explanation for this willingness to ‘over-share’ lies in the ‘blurry edges’ that characterize social networks. She points to the telephone directory as a historical example of a rudimentary social network – while generally individuals do not wish to

---

265 Ibid.
266 Ibid.
268 Ibid.
receive calls from people they do not know, most people traditionally have their phone number listed; “the social cost of not receiving phone calls from someone you fail to identify a priori as being in your social network outweighs the harm of having to… hang up on telemarketers.”

This same calculation drives individuals to place information online – in declining to strictly password protect their images or other information, she argues that individuals are “taking advantage of the blurry edge” because they are unable to decide in advance all the people who will be in their social network. Gelman does admit that the latest versions of the online social networks, which allow for images to be shared only within certain groups within one’s larger network of friends, have “conquered the binary decision [of] whether to publish or keep private” certain information. However, she also contends that the corporations running the online networks have an incentive to “capture the economic benefits of user’s blurry-edged social networks”, and thus they continue to make it easier for users to ‘over-share’ rather than restrict.

Even if there are other factors at play, as Gelman and Kane suggest, I nonetheless accept that the disinhibition effect associated with online anonymity has at least some benign manifestations; indeed, one of the great advantages of the Internet is that it allows for individuals to experiment or ‘try on’ different identities and to try out role-playing in various ways, or to make political comment without fear of reprisal. All of those are psychologically and socially beneficial activities. Even the ‘over-sharing’ elements of which Kane and Gelman speak may have

---

271 Ibid.
272 Ibid.
273 Ibid.
positive aspects. But the online disinhibition effect can also manifests itself in far darker ways –
the rudeness, harassment, and even threats of physical violence described in the examples of the
operation of the human flesh search engine, for instance. More prosaically, anyone familiar
with the typical content of the online comment boards of any major Canadian newspaper will
recognize this phenomenon. I suggest that it this side of the disinsinhibiting effect of online
interac
tions that explains why public shaming that stems from Little Brother surveillance can be
so vicious and disproportional. The phenomenon is driven further forward due to the low (or
even zero) costs (both monetary and other) of anonymous online sanctioning. To return to the
esteem theory of norms, McAdams contends that as people compete with each other to be well
thought-of, the costs of noncompliance with a norm (being sanctioned) necessarily increase. As
people seek to avoid those costs, overall compliance increases. However, this in turn means that
the status gains from complying with the norm are not as great, since there are more people
complying, and so some individuals seek to “achieve high or ‘hero’ status by leading the way to
new and higher levels of norm compliance.”274 In other words, in order to separate themselves
out from the masses, ‘heroes’ seek additional status by demonstrating their commitment to the
norm through increasing levels of compliance, or obvious, visible compliance. But thanks to the
existence of secondary norms, which arise “when individuals lower their opinion of those who
fail to censure primary norm violators”275, the competition for hero status can also occur in the
process of sanctioning itself – a competition to increasingly sanction others, in order to receive
esteem for compliance with the secondary norm. This has the effect of ratcheting up the overall

274 McAdams, supra note 219 at 366.
275 Ibid.
level of sanctions as individuals compete to demonstrate their compliance with the secondary sanctioning norm – as more people reach the new level, ‘heroes’ must push on ever further.

In the offline context, the pressure to compete can reach levels where it “causes individuals to bear material costs to comply with secondary enforcement norms… people [will] bear costs to inflict material costs on norm violators.” Yet because they are still bearing costs, there will be at least some downward pressure on competition between individuals seeking to sanction others. In contrast, this safety valve does not exist online. The cloak of anonymity provided by their computer means those seeking to shame norm violators bear no increased costs for increasing levels of sanctioning, other than the time devoted to the enterprise. Given, then, that the relative costs of sanctioning through online public shaming are essentially zero, competition for ‘hero status’ amongst countless anonymous commentators encourages new and ever higher levels of sanctioning. This greatly increases both the numbers willing to sanction behaviour of which they disapprove and the intensity with which they sanction it, even when it in no way personally affects them – they may not even live in the same society, let alone have personal contact with the ‘violator’. In combination with the disinhibition effect, typical limits on the kind of sanctions that might be applied are removed (or rather, are never in place to begin with), and the process can quickly spiral out of control. This then can result in a ‘vigilante’ mentality and sanctions that are grossly disproportionate to the alleged infraction.

The revelation of truly abhorrent behaviour is not necessarily a bad thing, and thus far the more extreme cases of online shaming have occurred in the context of revelation of seemingly

---

276 Ibid.
criminal activities, such as the hunt for people engaged in animal cruelty, or paedophiles. Of course, the example of the Boston bombings also show us that the human flesh engine can get their targets horribly wrong, even if the supposed context (find a terrorist!) is presumptively valid. But we have also seen examples where the norm violation appears rather less serious, such as insufficient etiquette on public transit, or where the alleged ‘violation’ is nothing more than existing as a socially awkward teenager. What can explain these campaigns? We can return to the idea of bidding for esteem or group acceptance – it is possible that the norms seen to be being violated are not even ones that the sanctioners feel especially strongly about, but since the cost of sanctioning online is zero, it is conceivable that group members may “go along” with a sanctioning campaign simply because the benefits of doing so are increased group cohesiveness or enhanced individual esteem. The fact that geo-immersive technologies operate in an online environment means that one must be sensitive to the potential ‘ratcheting up’ of sanctions in the manner I have outlined, even for seemingly minor transgressions.

Sanctions Without Norm Transgression

Sanctioning, however, is not likely to be limited only to online campaigns conducted in response to clear breach of a social norm. There is a growing body of evidence that suggests individuals captured in geo-immersive imagery may be the subject of intense scrutiny, commentary, and shaming simply for ‘existing’. Voyeuristic commentary is often made upon the basis of gender, ethnic, or class-based lines. In particular, there is heavy focus on sexualized imagery of women across websites that archive ‘notable’ geo-immersive imagery, so that it may escape any takedown request; Figure 18 is merely one example of many.
Figure 18 – topless sunbather.  

Ericson and Haggerty’s postulation that surveillance can “reproduce sexualized objectifications through the gendered voyeuristic gaze” therefore appears to be holding true with this embryonic technology. Indeed, the entire “doxyspotting” archive, discussed earlier, can be linked to this kind of objectification – users are explicitly trying to find prostitutes within geo-immersive imagery, but of course, ‘prostitute’ ends up only being code for “a woman wearing a short skirt.” This phenomena is not unique to geo-immersive surveillance of course – Koskela has also argued that CCTV surveillance also reinforces gender disparities, where “women are

---

278 Ericson & Haggerty, supra note 75 at 15.
invisible as suspects and as victims, but are targets of voyeuristic use of cameras.”

Lyon too believed that “scopophilia applied to… the viewer society has been translated as a predominantly male gaze that depersonalizes women, turning them into objects to be looked at.”

Thus, geo-immersive surveillance is not unique in its objectification of women, but is replicating the ‘male gaze’ found elsewhere. That it is not unique, however, does not mean it is any less harmful.

The scrutiny being applied to geo-immersive imagery is not limited to sexual voyeurism, however. Images can (and are) also be ‘cherry-picked’ in order to confirm various stereotypes. Is the young Briton in the Figure 19 vomiting because he’s drunk, or vomiting because he has food poisoning? One online commentator concluded that it indicated British youth in general were “drunk, jobless, and [with] demonstrably declining IQ”) and that the man was drunk, despite no presence of alcohol in the picture.

---

279 Hille Koskela, "Cam Era' -- the Contemporary Urban Panopticon" (2003) 1(3) Surveill Soc 292 at 301.
280 Lyon, supra note 189 at 48.
Are the young black men gathered around a car in Figure 20 chatting with friends or engaging in a drug deal? The viewers of the picture online concluded that clearly they were witnessing a narcotics transaction, despite the complete absence of drugs in the image.\textsuperscript{283}

\textsuperscript{282} Ibid.
While not an example of geo-immersive technologies but nonetheless a form of digital visual scrutiny, there is also a website devoted to mocking digital photographs of the patrons of a retail chain perceived to be ‘downmarket’. These examples all go to show that “different populations are subjected to different levels of scrutiny” and said scrutiny “continue[s] to play an important role in establishing and reinforcing social inequalities.” Geo-immersive surveillance may continue to raise, therefore, “questions of social division, both between

---

284 http://www.peopleofwalmart.com/, online, last accessed Aug. 3, 2010. This is not, to be clear, an example of geo-immersive technologies, as it depends solely on images uploaded by visitors of the site, and the images are not drawn from public space but rather a private retail establishment. However, similarities exist – those featured in the images are unaware that an image of them going about their daily business has been taken, or that it is now circulating online, or that they are being mocked online, or that the owner of the website is profiting from those images.

285 Ericson & Haggerty, supra note 75 at 14.

consumers and non-consumers and along fault lines of gender and ethnicity.” There is little reason to imagine such fault lines will not continue to influence the way in which different populations experience the effects of geo-immersive technologies – different groups will experience different levels of exposure, mockery, or other forms of sanctioning.

These new technologies change the calculus of the possible risks of being captured in an unflattering image – the possibility of group-led sanctions or mockery is significantly lessened should an image only be recorded in a tourist’s private photo album, or even if one’s image were printed in a newspaper prior to the transition to web-based publication. Geo-immersive surveillance changes the calculation by opening up every image for anonymous comments and – for the reasons I have outlined – increases the possibility of calls for action that can be highly disproportionate and lead to ‘real world’ consequences. In doing so, widespread surveillance of public spaces through geo-immersive technologies and the associate ‘Little Brother’ scrutiny of the generated images is likely to significantly increase both the quantity and quality of the kind of social pressure an individual is likely to feel. This is true both for those captured in clear breach of a social norm, but also of those who simply ‘exist’ in a manner that the anonymous crowd finds to be different, intriguing, tilllating, laughable, etc.

Is Geo-Immersive Surveillance Leading to Increased Social Sanctions?

In fairness, the above is largely a predictive exercise, drawn from a limited set of examples. A more practical question, then, relates to the actual probabilities of sanctioning stemming from the viewing of imagery generated by geo-immersive technologies. However, evidence of

---

287 Lyon, supra note 2 at 157.
irregular or limited sanctioning should not lead one to dismiss concerns out of hand, since one of the difficulties with enforcement is tied to the nature of norms themselves. Just as norms are “coarse grained instruments”, enforcement too is “bound to be sporadic and uneven; equally bad violations of the norm will attract unequal penalties.” Interestingly, there are already examples of sanctions being applied against those who decline to participate in geo-immersive surveillance programmes: some Germans who opted out of street surveillance by Google (meaning their property was automatically ‘blurred’ upon publishing, an option Canadians currently do not have) found their homes and businesses ‘egg bombed’ by unknown individuals, who also left messages reading ‘Google is cool’ painted on their victims’ mailboxes. The fact that one can be publicly sanctioned (and even have one’s property damaged) by fans of a corporation simply as a consequence of declining to participate in a commercial public surveillance programme helps to further illuminate that even the mildest actions one takes in the virtual realm can have disproportionate consequences in the physical.

While there are not yet examples of the human flesh search engine being turned against individuals captured by geo-immersive technologies in an effort to exact punitive consequences in an offline context, the examples discussed herein are evidence that judgments are being made about images online, suggesting at least that the potential is there. The shaming, mockery, or outright voyeurism is done not only on the original geo-immersive website, but also on websites that host collections of images taken from Street View or comparable services that are deemed ‘noteworthy’, out of the reach of the take-down notices of the original geo-immersive

---

288 Arneson, supra note 221 at 35.
technology providers for the reasons I have already explained. While admittedly there are currently only a limited set of examples upon which to draw, that is because these technologies are still in their infancy. Thus, while the odds of being captured in an image for any one person are currently relatively low, unchecked growth and use of geo-immersive technologies will mean those odds may dramatically shift in the future. Simply because there is not already a very large set of examples of social sanctioning in the context of geo-immersive imagery does not mean that the potential does not exist, nor does it mean we ought to wait for that growth before implementing the necessary regulatory changes to cope with the societal changes it may bring.\textsuperscript{290}

The Possibility of Positive Norm Reinforcement

In this section, I have argued that the online disinhibition effect that characterizes many digital interactions may lead to the over-zealous enforcement of sanctions for comparatively minor norm transgressions. As I have admitted, however, this is largely a predictive exercise based upon a relatively small set of examples. There is also the possibility, then, that the online disinhibition effect might also lead to the strong enforcement of a more positive set of norms. For instance, it might be deemed socially unacceptable for digital communities to attempt to identify individuals captured in images, and this norm might be policed by members of that community for the same ‘group cohesiveness’ or ‘esteem’ reasons I earlier outlined. Indeed, the phenomenon of “doxxing” suggests that is at least partially the case in certain digital communities. Doxxing (not to be confused with doxyspotting), refers to the posting of personal information about individuals; sometimes the individuals are anonymous and the doxxing ‘outs’

\textsuperscript{290} See this Chapter at heading “A Legal Response: When, and Against Whom?”.
their actual identity, and sometimes the individuals are already known and the ‘doxxers’ seek to discover and share extremely detailed personal information about them. While ‘doxxing’ originated out of digital communities, there some who have rejected it, arguing that seeking to connect one’s identity online to one’s real-world identity is a fundamental betrayal of their values. For instance, in the MetaFilter digital community, the ‘doxxing’ of a fellow member or attempting to harness the community to participate in the ‘doxxing’ of a non-member will result in a permanent ban.

Beyond the ‘doxxing’ context, there have been examples of digital communities turning against those members who attempt to shame individuals caught in an image that has been widely shared. In a recent example, a member of Reddit surreptitiously took a photograph of a Sikh woman, uploaded it to Reddit, and mocked her for her appearance. While some joined in with the mockery, other members of the community criticized that user for failing to understand the Sikh view of body hair. The image was shared widely enough that the subject herself was made aware, leading her to comment on the photo explaining the importance of her religion in her life. This ultimately led to the photographer apologizing:

I've read more about the Sikh faith and it was actually really interesting. It makes a whole lot of sense to work on having a legacy and not worrying about what you look

---

294 “I’m not sure what to conclude from this”, Reddit, online, [http://www.reddit.com/r/funny/comments/109cnf/im_not_sure_what_to_conclude_from_this/?sort=new#c6bmnym](http://www.reddit.com/r/funny/comments/109cnf/im_not_sure_what_to_conclude_from_this/?sort=new#c6bmnym), last accessed May 24, 2013.
like. I made that post for stupid internet points and I was ignorant. So reddit I'm sorry for being an asshole and for giving you negative publicity. Balpreet, I'm sorry for being a closed minded individual. You are a much better person than I am. Sikhs, I'm sorry for insulting your culture and way of life. Balpreet's faith in what she believes is astounding.295 [sic]

This suggests the possibility that certain norms might emerge as geo-immersive surveillance spreads that combat the identification or shaming efforts of the human flesh search engine, or that norms against ‘overreach’ in the shaming of others may also emerge. It seems likely that there will be competing norms across different digital communities. Just as certain communities enthusiastically embrace ‘doxxing’ as a method of enforcing social control and some reject it, the same is likely to be true in the context of geo-immersive technologies – some communities will refuse to participate in shaming campaigns, while others will enthusiastically get on board. Again, because this is simply a predictive exercise, it is difficult to anticipate exactly how norms will evolve in a world characterized by frequent geo-immersive surveillance, but I do acknowledge the possibility that competing norms might arise that combat at least some potential for the occurrence of the harms I have identified in this Chapter.

The Potential Effects on Behaviour & Norm Transmission

In the previous section I explained the function of social norms in society, and considered the ways in which breach of those norms can be sanctioned. I suggested that geo-immersive technologies create the potential for anonymous scrutiny of the generated images, and that the human flesh search engine may be harnessed to hunt out behaviours that are deemed to be

transgressive, but also those that are simply surprising, titillating, interesting, or otherwise of note. In this way, sanctioning may occur not only in the context of revelation of ‘shocking’ behaviours that violate a well-established social norm (i.e. public urination), but also far more mundane activities (i.e. the example of the young men gathered around a vehicle and conversing). I provided examples of how the human flesh search engine operates, arguing that its origins in anonymous online communities help explain how shaming can quickly spiral out of control, and can even lead to physical violence in the offline world. I showed that we are already beginning to see examples of judging behaviour by anonymous communities when they scrutinize and share images generated by geo-immersive technologies, and it is my contention that as the use of such technologies becomes more widespread and common, the more images will be available for scrutiny. In turn, this will significantly increase the probability that individuals captured in them will be subject to online campaigns of shaming and other forms of harassment.

However, I wish to now consider less the direct effects that such digital shaming can have on specific individuals who have their activities revealed, and more the broader effects that may affect anyone who lives in a society subject to the kind of everyday surveillance represented by the increased use of geo-immersive technologies, regardless of whether they are personally captured in an identifiable image. In this section and the next I intend to consider the question of whether geo-immersive surveillance might lead to the adoption of certain norms, either through conscious anticipatory conformity in order to avoid the kinds of sanctions discussed in the previous section, or the unconscious internalization of those social norms by simply living in
a society characterized by the possibility of random, enforced exposure of one’s public activities to an audience of potentially hundreds of millions. While on one level this may seem to be no bad thing (indeed, who is in favour of increasing the numbers of ‘Dog Poop Girls’?), the same process that may correct genuinely anti-social behaviour can also privilege either certain sets of social norms, exposing those who ‘violate’ them to ridicule and danger.

Anticipatory Conformity

A desire to avoid sanctions or reputational harms may lead to conformity “when perceived or real pressure from others causes us to act differently from how we would act if alone.”296 Such conformity might take two forms – it could be actively “conforming to contrary positions [from one’s own preferences]” or it could be “conformity by omission, that is, failing to behave in a certain way because the group would not approve of such behaviour.”297 Such an effect is well established in the surveillance literature. It is my contention that the Little Brother style scrutiny associated with increased use of geo-immersive technologies may lead to either form of conformity. In both cases, it can be a kind of anticipatory conformity – rather than altering behaviour in response to a sanction for violation of a social norm, behaviour is altered to avoid being sanctioned in the first place. An underlying principle of such anticipatory conformity in the context of surveillance is that, essentially, “observation alters conduct.”298 The Privacy Commissioner of Ontario, for instance, has described surveillance as having a “chilling effect on [an individual’s] freedom to speak, act, and associate with others… since individuals may censor their own activities when they are aware of being watched, [such] surveillance may also

296 Cialdini & Trost, supra note 209 at 162.
297 Ibid.
be perceived as a means of enforcing social conformity.” In Cockfield’s example for instance, “if an individual thinks that [her] impromptu ‘Singing in the Rain Dance’ in a downtown centre will somehow be stored and potentially used against her in the future, she may change her behaviour and in doing so edit her expression.” Anticipatory conformity is not simply a matter of avoiding truly abhorrent behaviour; rather, where surveillance causes the potential for significant overreaction by third parties, it may lead individuals to alter an entire range of behaviours.

The structural aspects of geo-immersive technologies enhance its potential to lead to anticipatory conformity. In a world in which widespread geo-immersive surveillance is absent, individuals can reasonably assume that when undertaking activities in public they will be exposed only to those who are physically and temporally present. Moreover, they are generally able to reasonably calculate the risk of exposure to large groups of people beyond those present with relative accuracy. For instance, in ‘everyday’ situations, one would reasonably assume that the possibility of one’s image being surreptitiously recorded and distributed to a global audience is negligible, while if one attended a public rally or televised sports event, one ought to expect that there is an increased possibility that identifiable images might be beamed to televisions across the country or even around the world. Similarly, even if photographed on a public street by a tourist, one might reasonably expect that the resulting image would be shared with comparatively few individuals, rather than becoming part of a globally accessible archive.

---

While there are always exceptions – what happens if one is caught up in a newsworthy event, or happens to be on the street in the vicinity of a documentary filmmaker – in general people in public space retain a relatively effective ability to predict the limits of their exposure.

The ability to make such a calculus also means that individuals can make a conscious choice to demonstrate a certain set of (possibly contrarian) social values or norms to those who are present, and thereby make a choice to be part of a public dialogue about those values or norms if they wish. Individuals may choose, for instance, to intentionally violate certain behavioural norms in public and risk public sanction, in order to make a statement about the value of the social preferences they hold. But such demonstrative activities done in public still remain a conscious choice – individuals can choose to act in public in a deliberate manner, knowing full well that they will be observed while doing so, and willingly accept the possible consequences. The decision remains theirs and theirs alone. In contrast, a widespread system of geo-immersive surveillance would potentially disrupt the ability of individuals to make an informed calculation about exposure in ‘everyday’ circumstances. It would force exposure in the sense that it is not generally plausible for an individual a modern society to exist without ever being ‘in public’.

While it is true that geo-immersive service providers do not directly force individuals to submit to being imaged, there is no mechanism for an individual who sees a camera-equipped car on the street to instruct the driver to turn the cameras off. This is compounded by the fact that the collection of imagery tends to be accomplished in a relatively discrete manner, often with the result that the information is gathered without even the knowledge of the photographed – the Street View cars (again, as a paradigmatic example) appear from distance as any other car
might, and it would take a keen eye to spot the camera attachment when the vehicle is moving at speed – and this is only even a possibility if the individual happens to facing in the direction from which the car is approaching. Indeed, even if it were spotted, it is probable that many people would have no idea what it was. To reiterate, I accept that the chances of being imaged by geo-immersive technologies are currently low, but even now these risks are emerging, thanks to the lack of sufficiently detailed advance notice\(^{301}\) of when imaging will occur. When one cannot predict with certainty when a sanction may be applied, who may apply it, or what it may be applied for, the safest approach may be to alter one’s behaviour across a wide range of activities, at all times. The possibility of having public activities exposed to groups removed in both time and space from the site of the actual behaviour itself may result in individuals avoiding or modifying a range of behaviours in public that they are concerned may lead to opprobrium from the anonymous crowd. In a nutshell, this is the potential for anticipatory conformity to particular social norms in the face of geo-immersive surveillance.

Of course, it is commonplace to try and avoid sanctions from one’s peers by conforming to social norms, and this can be entirely innocuous – bringing a bottle of wine to a dinner party, for instance. Likewise, it is necessary here to again make the same caveat made above – it is possible that ‘positive’ norms might spread, and that some choose to ‘anticipatorily conform’ to them out of fear of sanction should be greeted with satisfaction rather than concern. Once again, we are in the realm of speculation and it is difficult to predict exactly which norms will benefit from increased visibility thanks to geo-immersive surveillance, but I think caution should be raised for at least two reasons. First, as explained any associated sanctions may be

\(^{301}\) I will explore the issue of ‘notice’ in greater detail in Chapter 7.
disproportionate, and may therefore lead to conformity not out of a positive desire to perform a particular social role or maintain desired relationships, but rather out of fear. Second, the conformity may be conformity to the norms of a group of which the targeted individual is not a member. This is particularly problematic in the context of a pluralistic society – it is one thing for cultural (or other) groups to seek to enforce social or cultural norms within that particular group, but it is something different to have one group attempt to enforce its norms on another, unrelated group. In the next section then, I want to consider the direction that conformity might take in the context of changes in behaviour stemming from geo-immersive surveillance. I suggest it will likely be conformity towards the social norms held (or apparently held) by the cultural majority or otherwise dominant segment of the population.

**The Privileging of Cultural Majorities**

Countless groups would surely prefer that their legal, publicly undertaken activities nonetheless not be broadcast to a global audience. Patients attending psychiatric offices, teenagers entering abortion clinics, cheating spouses entering hotels, employees going to a meeting at the office of their employer’s competitor, street protesting in favour of an unpopular political party – all of these activities are legal, if of varying moral acceptability by societal majorities, and thus all are those kinds of activities that the individuals in question might wish to keep largely hidden from public view. What geo-immersive technologies do is create the chance that rather than having those activities only exposed to the small number of individuals actually present spatially and temporally, they are exposed to the scrutiny of a much larger audience. The fear of being caught undertaking an action seen as transgressive or even merely undesirable may lead individuals to habitually or unconsciously conform their behaviour in public spaces to what they
perceive as the most dominant social norms. Conformity to social norms is widespread – psychologists have conducted experiments that suggest in the absence of an objective rule for behaviour, individuals are most likely to “behave according to the group consensus.” This is the situation that is of primary interest to this thesis – as noted, I am not particularly concerned with the public sanctioning of acts animal cruelty (other than questions of proportionality), because that is sanctioning for violation of an objective rule of behaviour (a law). Instead, I am more interested in the sanctioning that occurs when there is no such objective rule of behaviour on a given subject. While the expanded use of geo-immersive technologies may encourage uncontroversial conformity to dominant norms that overlap with objective rules/laws of behaviour, such as prohibitions against animal cruelty, there is little to stop that conformity from also expanding more generally across a wide-range of social or behavioural norms.

Indeed, the actions of online communities have already extended into sanctioning people for completely legal behaviour (for instance, questions of social etiquette) undertaken in public or quasi-public space. The range of norms that can potentially be enforced is, however, naturally limited by what can be gleaned from any given image. This is one reason I will argue in Chapter 8 for regulation limiting geo-immersive technologies to ‘still’ imagery rather than video – video surveillance gives a far greater chance of identifying particular behaviours than does a single snapshot. On the other hand, this technical ‘built-in’ limitation to still imagery has little relevance where the social shaming or mockery is the result of the subject simply being part of a particular socio-economic, racial, cultural, or other group found noteworthy by the sanctioners. For instance, as I earlier discussed, there appears to be a regular emphasis on the search for (and

302 Cialdini & Trost, supra note 209 at 155.
archiving of) images of women, particularly in quasi-sexual circumstances. Sanctioning or mocking is not, then, *always* dependent on breach of a social norm. In such cases, the shaming may be understood as a regular affront to dignity – the message is that one is less worthy or is deserving of shame simply by one’s membership in the identified group. Since individuals in such circumstances are not actively breaching a social norm, it is more challenging to argue that they are likely to ‘conform’ their behaviour to said norm. Instead, it is best understood as the ‘internalization’ of their status as objects to be shamed, mocked, or sexually desired in the eyes of the viewers, rather than as active agents. I will argue later in this Chapter that anticipatory conformity is likely to ultimately lead to the internalization of social norms in a way that has negative consequences. In the context of shaming for group membership, this same process can occur, without the need for behavioural change to avoid sanction. Rather, the internalization is of one’s status as an object rather than subject. This is directly connected to the way in which geo-immersive surveillance may serve to privilege existing cultural majorities or socially dominant groups.

Conformity generated by sanctioning or mocking may be in the direction of *majority* social norms, even if it is in fact a relatively small number of ‘Little Brothers’ conducting the scrutiny. It appears as though - at least in Western nations – that the participants in the digital communities that appear most predisposed to conducting shaming campaigns are primarily drawn from majoritarian or socially-dominant groups. The individuals that spend time seeking out apparently norm-violating behaviour in images viewable online tend to be young, male, and digitally well connected. Figure 21, for instance, represents the reported demographics of users
of 4chan by the online measuring service Quantcast in November of 2010. Over half the users are located in the USA, 75% of them are male, 80% are white, and 70% are between the ages of 13 and 34 – a tiny minority (though a significantly powerful one) of the global population as a whole, only 5% of which is located in the USA and 51% of which is male.

These statistics suggest that social norms arising from particular digital communities are not necessarily going to be representative of a broad cross-section of a given population. If we consider this on an international scale, it will also tend to privilege the social norms of those residing in developed, digitally-connected countries – as of 2013, approximately 34% of the

---

303 Source: [http://quantcast.com](http://quantcast.com), last accessed Apr 18, 2011.
world’s population used the Internet,\textsuperscript{304} and “the [digital] gap between developed and developing countries has continued to widen since the 1990s.”\textsuperscript{305} While it is not certain that all online communities that participate in the scrutiny of geo-immersive imagery will share these characteristics, the evidence I have provided so far about the kinds of imagery that is “redistributed” beyond the initial service provider would indicate that young, white men are the primary drivers. If the sanctioning led by these digital communities is towards compliance with the social norms of that group, then it is clear that the potential for mockery, shame, or vilification is far greater for certain minority groups than it is for others.

Thus, even if there is no broad social consensus in the offline world that those groups are deserving of such attention or shame, minority groups seen as ‘easy targets’ might find it particularly difficult to maintain their other-regarding norms in the face of concentrated pressure. Digital shaming campaigns led by a narrow strata of society may therefore pose a particular threat to such communities, which may often have different social norms and preferences. Thanks to the online disinhibition effect, geo-immersive technologies may have the unwanted (but serious) consequence of subjecting those communities to intense social sanctions that pressure them in the direction of adopting majoritarian norms (or whichever norms the narrow strata ends up favouring).\textsuperscript{306} As McAdams notes, “the esteem model predicts the widespread existence of nosy norms by which majorities enforce their other-regarding

\textsuperscript{306} I argue in the next section that this has the potential to subsequently influence private behaviours too (see heading ‘The Potential for Panopticism & the Internalization of Norms’).
preferences on minorities.”\textsuperscript{307} Because the cost of imposing esteem penalties is low, “they make it privately worthwhile to enforce rather weak other-regarding preferences [and] the result may be to deter socially valuable behaviour.”\textsuperscript{308} There is no reason to believe this theory will not hold in the context of sanctions led by digital communities for perceived social norm violations captured in geo-immersive imagery.

Of course, there is also a counter-argument to concerns that geo-immersive surveillance will lead to anticipatory conformity towards the norms of either the majority or digitally literate minority. Geo-immersive technologies may also provide a window into minority behaviours, helping to ‘normalize’ them in the mind of the viewing public. It might be argued that geo-immersive technologies contribute to permeability of community boundaries, allowing for increased cultures of tolerance as exposure increases. Similarly, an argument could be made that an individual with a desire to follow minority norms but living in a majority neighbourhood may feel reassured and strengthened by virtue of discovering online the existence of communities that support the very values she feels she must hide. Those with minority political opinions may come to discover the existence of an entire movement in another city devoted to the same cause, proudly and knowingly undertaking street protests in full view of both passing members of the public and cameras. So, I do accept that geo-immersive technologies have the potential to form a new and interesting part of that cross-cultural conversation, and in considering the possibility of enforcement of majoritarian social norms against an unwilling

\textsuperscript{307} McAdams, \textit{supra} note 219 at 426.
minority then, we must also be conscious of the possibility that geo-immersive technologies may have an important levelling impact, thereby increasing tolerance rather than decreasing it.

However, in the context of the (effective) zero-cost of online sanctions, it is my suggestion that even strongly held norms by minority communities may weaken under the threat of the sustained pressure that can be associated with online shaming and sanctioning. Geo-immersive technologies, widely implemented, would dramatically raise the possibility that groups with contrarian, risqué, or merely unpopular social norms or behavioural preferences would suffer increased opprobrium for their public activities, increasing the possibility that they begin to modify their behaviour in order to avoid sanctions. Moreover, while such conformity may initially alter only public behaviour, I will argue in the following section that in the face of constant surveillance (be it real or merely perceived), it is possible that those subject to intense scrutiny might ultimately internalize certain norms. When that occurs, not only is public behaviour altered, but rather private behaviour too, homogenizing cultures in a way that may be contrary to the interests and goals of a pluralistic, diverse society.

The Potential for Panopticism & the Internalization of Norms

I argued in the previous section that increased scrutiny of images generated by geo-immersive technologies, along with sanctions for any perceived norm violations in those images may lead to a process by which individuals, especially those from minority communities, modify their public behaviour. However, as Hetcher argues, “conformity is not necessarily a conscious or

309 Cialdini & Trost, supra note 209 at 162.
310 Of course, this is predicated on the notion that diverse, pluralistic cultures are inherently a good thing. There are those, of course, who would argue that a largely homogenized culture is likely to be more stable and peaceful. Such arguments are, however, beyond the scope of this thesis.
intentional process – one may track the behaviour of others without being conscious that one is doing so.” In this section then, I wish to consider this possibility – that simply living in a society characterized by enforced exposure of public activities to an unknown, anonymous audience may cause unconscious conformity with – or internalization of – majoritarian norms. If such internalization occurs, then it may begin to be reflected in private behaviour as well. Not all norms are necessarily internalized – Geisinger notes that social norms “may or may not be internalized”;³¹¹ McAdams concurs though adds that internalization “obviously occurs and [can] provide an explanation for behaviour.”³¹² When a norm is internalized, individuals are no longer simply intentionally avoiding sanction in the manner of anticipatory conformity, but rather are unconsciously modifying their behaviour. The consequence of violating a norm one has internalized may be felt as ‘guilt’, or as Strahilevitz explains, “an individual may conform to a norm because her self-esteem depends on her compliance with it.”³¹³

In the surveillance literature, intense, focused visual surveillance is often considered to lead to the possible internalization of norms. Surveillance, after all, “is a powerful technology for social control.”³¹⁴ This control is often described as ‘panoptic’ – Bentham’s Panopticon was a proposed prison model in which each inmate was constantly viewable by a centralized administrator, though they could not see whether or not the overseer was in fact monitoring them at any given time. Bentham theorised that such a system would result in as much obedience by the prisoners as if they were in fact being watched at all times, and would

³¹¹ Geisinger, supra note 216 at 608.
³¹² McAdams, supra note 219 at 380.
³¹³ Strahilevitz, supra note 215 at 537.
therefore be cheaper to operate, requiring fewer supervisors to ensure obedience to the rules from the same number of prisoners. Foucault considered the model of the Panopticon in *Discipline & Punish*, suggesting that the unequal gaze central Bentham’s model was the hallmark of many modern disciplinary systems – not just prisons, but any institution with a central authority, whether it was a hospital, school, or factory. Bentham’s model was based upon an ‘inspector’ who not only laid out the directives for behaviour, but also stated the punishment for violation, and ultimately enforced the punishment if necessary. Foucault’s great insight, however, was that under the right circumstances, the power of the gaze meant that the inspector in fact became unnecessary:

The effect of the Panopticon [is] to induce in the inmate a state of consciousness and permanent visibility that assures the automatic functioning of power. So to arrange things that the surveillance is permanent in its effects, even if it is discontinuous in its action; that the perfection of power should tend to render its actual exercise unnecessary; that this architectural apparatus should be a machine for creating and sustaining a power relation independent of the person who exercises it; in short, that the inmates should be caught up in a power situation of which they are themselves the bearers [emphasis mine].

In other words, individuals subject to panoptic power no longer need to be regulated, for they regulate themselves. Foucault contended that individuals within such settings participated in their own control by internalizing the rules in order to avoid punishment; the purpose of the unequal gaze was “to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power.” Solove argues that surveillance of this sort is

---

316 Ibid.
317 Koskela, *supra* note 171 at 300.
318 Foucault, *supra* note 315 at 201.
both “subtle [and] pervasive… it changes the entire landscape in which people act, leading
toward an internalization of social norms.”

Can it be said that the scrutiny associated with geo-immersive technologies has the potential to generate the kinds of behaviour conforming qualities associated with panoptic institutions? In my view the answer is generally yes, though there are important distinctions to be drawn. The Panopticon, for instance, is a top-down concept, which tends to reduce all fears of observation to the fear of the single over-seer, in the mould of Orwell’s “Big Brother”, watching to ensure we stay in line at all times. Bentham’s original model of the Panopticon was the prison, while Foucault spoke more generally of systems characterized by discipline and punishment – any institution that sought conformity of behaviour. In the Panopticon (as traditionally understood), it is the fear of observation and subsequent punishment for transgressive behaviour that leads to conformity with the directives of the unseen administrator; “you never know when the inspector’s eye will be on you, so you modify your visible behaviour in order to avoid negative sanctions.”

Although Foucault realised the logic of the Panopticon extended beyond the prison gate, he still considered it a tool of administration, making bodies docile for the purposes of control. This has led to criticism of an over-reliance or over-generalization of Panoptic theories, since, as Lyon describes it, “Foucault’s perspective seems to revolve around the concept of power in a way that almost excludes other proper sociological conditions; power, expressed as domination or violence, is almost all there is.”

Geo-immersive surveillance, in contrast, has a ‘pleasure’ quality to it, a characteristic not typically associated with panoptic

---

319 Solove, supra note 174 at 35.
320 Lyon, supra note 189 at 44.
321 Lyon, supra note 2 at 26.
institutions. As Haggerty puts it, “both watching others and being watched can at times be pleasant entertainment activities… [and this] does not fit neatly within the preoccupations of the Panopticon.” The most significant challenge posed by geo-immersive technologies to typical panoptic theories, however, is that the role of the overseer no longer exists in a way contemplated by either Bentham or Foucault. As I have argued, the bifurcation of the surveillance infrastructure means that even though the collection of geo-immersive imagery is relatively centralized (at least, on a ‘per provider’ basis), the ‘overseers’ are utterly unconnected to that collection or the individuals caught by it.

However, even though the structure that typically characterizes panoptic institutions is lacking, important insights about how individuals may alter their behaviour under conditions of observation can nonetheless be retained. Indeed, this is true in the context of much modern consumer surveillance, where centralized administration or attempts to control are not the issue – there are multiple competing entities conducting overlapping forms of surveillance. As a result, the Foucauldian “vision of control is no longer operational in the overwhelming majority of contemporary environments where collective interaction takes place.” Surveillance scholars seeking to apply these lessons to the more diffuse surveillance of cities therefore often describe it not as panoptic, but rather ‘polyoptic’, ‘synoptic’, or ‘superpanoptic’. These theories do not necessarily reject the core insight of Foucault’s approach to the Panopticon,

---

322 Haggerty, supra note 286 at 28.
325 Haggerty, supra note 286 and Lyon, supra note 2.
326 Lyon, supra note 160.
however. Instead, they argue that while the panoptic effects *may* be stronger when the surveillance is state-run or centralized in some fashion, more diffuse systems (such as independent networks of CCTV cameras run by multiple corporations) may nonetheless have significant and measurable effects on the behaviour of those being watched. Bogard, for instance, contends that the social control possibilities associated with the Panopticon still have meaning beyond the disciplinary institutions in which they arose – in the modern context, he argues that the control is simply “disarticulated… no longer organized by hierarchy or centralized power.”

I concur with polyoptic theorists that such control does not necessarily have to have a central active source – it can be diffuse yet still powerful. Thus, the fact that the “inspectors” in the context of geo-immersive surveillance are dependent on a separate organization for the imagery should not meaningfully alter the possibility for norm internalization. As Koskela describes it, “the panoptic condition of video-surveillance imposes self-vigilance [and] the internalisation of control.” As a result, it doesn’t really matter *who* is doing the surveillance – “it could be a computer and it would make no difference.” Individuals who exist in a state of persistent or regular visibility to recording devices live in an environment where their behaviour can be shaped “not so much by the threat of punishment and physical force but by the act of being watched.” Consequently, while the surveillance effected by geo-immersive technologies may

---

328 Koskela, *supra* note 171 at 253.
329 Koskela, *supra* note 279 at 302.
be “less invasive and more reliant on technology” than the kind that is typically associated with
the disciplinary institutions of the Panopticon, it is “equally capable of effecting significant
psychological and behavioural changes… the very possibility of an observing gaze produces
changes in the behaviour of the observed.”

As Fairfield puts it, “the lesson of the Panopticon is that persons who experience themselves as being completely visible inevitably succumb in
large and small ways to imperatives of normalization and social conformity.”

While I have argued that widespread surveillance is more likely to have these harms, it need not
be characterized by permanent camera installations or video surveillance to reach this threshold
of forcing people to feel “completely visible”. Foucault teaches us that the internalization of
norms can occur even when the surveillance is not constant – even though the gaze created by
even widespread geo-immersive surveillance may not be permanent in the manner of the prison
tower or systematic in the fashion of a citywide network of CCTV cameras, the inability of
individuals to accurately predict when they might be captured in an image and by whom they
might be subject to online shaming means that Panoptic style internalization of norms remains a
distinct possibility. Once a certain critical mass is reached of competing geo-immersive
providers such that there are regular occurrences of shaming for ‘revealed behaviours’,
individuals may grow to feel as though they are constantly under watch, even when they are not.
If this occurs, then the conformity may not only be in public space as a conscious decision to
reduce the risk of sanction, but also behind closed doors as a result of unconscious norm
internalization. Conformity that is internalized is conformity that is complete, and this is

331 Karas, supra note 72 at 44.
332 Fairfield, supra note 34 at 46.
problematic not only for minority groups, but for the wider community too. At a certain point, internalizing these rules and social norms will mean that there is no longer any need for them to be explicitly enforced by the Little Brothers or anyone else, and the ‘soul training’ of Foucault may become a reality.

The Public Harm of Norm Internalization

Conformity to social norms is to some extent, of course, necessary – ‘society’ is predicated at least in part on large numbers of people agreeing to appropriate behavioural standards. Society with no behavioural conformity whatsoever would be chaos. But while some conformity to social norms is inevitable, and even desirable at times, the concern raised in this thesis surrounds the consequences for society when enforced public exposure serves to privilege certain sets of norms over others, by magnifying the power of sanction for breach. Norm internalization is not, however, only potentially harmful for minority groups, but for society as a whole. As Phillips suggests, the protection of “subcultures benefits more than the members of that subculture – it also acts as a public good, contributing to a diverse, vigorous, vibrant, and evolving civic life.”333 It is irrelevant that the Little Brothers spoken of herein may have no intent beyond mockery or shaming of particular individuals they deem ‘worthy’ of such treatment. The sum of those actions is greater than their parts, for, as Haggerty argues, while the repression of public debate “can be the explicit aim of conducting surveillance… it can [also] be an unintended by-product of monitoring.”334 A widely deployed system of geo-immersive technologies, then, may cause conformity to or internalization of certain dominant

norms in a way that not only affects members of minority communities, but of society as a whole, changing the nature of public space through unpredictable enforced exposure to an unknown anonymous audience. Since public space is “constituted through social action… the interactions that occur in that space”, any shift in the kind of interactions that occur within that space necessarily also changes its function and meaning.

One of the many functions of public space is to be a zone in which individuals can come together and freely participate in activities with like-minded souls, sometimes protected by the anonymity of the crowd or by being visible only to those physically present at the gathering. In this way, public space has a dual, but paradoxical, character – on the one hand, it is comprised of places we can go to in order to escape loneliness or avoid solitude, but on the other hand, those same places can also offer the chance to blend in with a group rather than being noticed individually. Westin has argued that this is a form of privacy that exists in public:

Anonymity occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance. He may be riding a subway, attending a ball game, or walking the streets; he is among people and knows that he is being observed; but unless he is a well-known celebrity, he does not expect to be personally identified and held to the full rules of behaviour and role that would operate if he were known to those observing him. In this state the individual is able to merge into the “situational landscape.” Knowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom that men seek in open spaces and public arenas.

Widespread geo-immersive surveillance may, however, reduce the possibility of ‘merging into the situational landscape’, and this would harm not only those minority groups with contrarian values, but may also stultify the growth of society more broadly; the promise of anonymity

336 Westin, supra note 62 at 31, cited in R v Ward supra note 53 at para 73.
while in public “promotes freedom of action and an open society… [whereas] lack of public anonymity promotes conformity and an oppressive society.”\textsuperscript{337} Indeed, the Ontario Court of Appeal recently acknowledged that “a degree of anonymity… is essential to the individual’s personal growth and the flourishing of an open and democratic society.”\textsuperscript{338} Unmonitored public spaces, especially in urban contexts, are places of “stimulation, of excitement, and of the cross-fertilization of customs, styles, ideas, and practices.”\textsuperscript{339} If, however, increased scrutiny through geo-immersive technologies causes people to begin to fear that their public activities may be exposed to an unknown, far-removed audience, this may change.

As Steeves contends, “there is an unwillingness to accept surveillance in voting booths and in public fora because, even though both involve participation in a public process, being watched in those circumstances severely restricts the individual’s autonomy.”\textsuperscript{340} Subject to surveillance, the public square will become increasingly homogenised in terms of those who feel comfortable demonstrating their values and beliefs in public. Increased surveillance of public spaces, therefore, may have the effect of “segregate[ing] and polari[zing] it… mak[ing] it less lively and spontaneous.”\textsuperscript{341} Regular or persistent surveillance through the scrutiny of geo-immersive imagery may serve to change the character of public space, ironically by making it more public – viewable to individuals anywhere, any time. If enforced exposure causes interactions in (physical) public space to be homogenized, the vitality of public sphere as a locus of creativity,

\begin{footnotesize}
\begin{enumerate}
\item[337] Christopher Slobogin, "Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity" (2002) 72 Miss LJ 213 at 236.
\item[338] \textit{R v Ward}, supra note 53 at para 70.
\item[339] Lyon, \textit{supra} note 160 at 67.
\item[341] Koskela, \textit{supra} note 171 at 294.
\end{enumerate}
\end{footnotesize}
diversity, and spontaneity, may also be harmed; by public sphere I mean “the space of civil society, as distinct from private association on the one hand, and institutionalized political society on the other.”

Not eliminated, to be sure, because interaction within the public sphere can occur in all manner of ways – beyond activities in public spaces, participating in the public sphere certainly includes essentially ‘private’ activities such as an individual writing to her newspaper from the privacy of her own home, publishing a blog online, or organizing meetings of like-minded individuals. Still others, naturally, will have no fear of speaking up in public regardless of sanction or rebuke they may receive for doing so. While history is littered with examples of brave individuals who do indeed stand up to such fierce sanction in a public display of their commitment to certain values, we should not require that as a litmus test of the validity of a particular belief. In the presence of monitoring, more and more the public square could be dominated by a particular set of values or a particular set of people, regardless of whether this is in fact an accurate reflection of society. The sharing and mixing of differing cultural values (something I take to be desirable in a diverse and pluralistic society such as Canada) is more difficult to achieve when individuals only feel comfortable demonstrating those values when in the company of those who already share them.

It is for this reason that intense surveillance of public space has been criticized as “hindering democracy, inhibiting the growth of representative institutions, corroding democratic traditions

---

and undermining patterns of sociability and trust that are essential preconditions for fostering
democratic practices."\textsuperscript{343} While such anti-democratic surveillance has typically been state-run,
any surveillance is properly labelled anti-democratic “to the extent that it prevents individuals
from coming together to identify common interests, forge alliances, and develop political
strategies.”\textsuperscript{344} Regan argues that if surveillance has the effect of revealing information about
one’s personal life to people who would not otherwise have ready access to it, then this might
also harm democratic participation:

Privacy may be essential to a democratic political system because some commonality
among individuals is necessary to unite a political community… the more people know
about the details of one’s personal life, the more individual or unique one is considered,
and the more difficult it is to construct a ‘public’ or community.\textsuperscript{345}

On the other hand, Regan’s contention is dependent on assuming that what people prefer not to
share is necessarily ‘unique’ – it could be the case, for instance, that revelation of personal
information actually shows that one shares much in common with your neighbour, rather than
less. A more compelling argument is, then, that democratic politics have relied at least in part
upon the importance of public association and a world in which only some are comfortable in
demonstrating their political values in public settings is one that necessarily must have less
scope for the transmission of political arguments, even if those arguments can still be made
‘online’ or in print. Effective democratic societies require the diversity of viewpoints that can
be generated from this kind of cross-fertilization as part of a robust public debate from which
the best ideas can be selected. I acknowledge and accept that geo-immersive surveillance is
unlikely to ever become as ‘intense’ as the kind associated with the monitoring of dissident

\textsuperscript{343} Haggerty & Samatas, supra note 334 at 4.
\textsuperscript{344} Ibid.
\textsuperscript{345} Regan, supra note 54 at 227.
political groups in authoritarian states. But while the kind of observation associated with geo-immersive technologies will certainly not eliminate public debate, it does threaten to hinder it in some aspects, and privilege certain groups over others in their ability to make use of public spaces – and thus the public sphere – in the furtherance of their goals, political or otherwise. There remains, then, “an inherent connection between autonomy, privacy, and democratic action.”  

Summary

I have argued in this chapter that widespread geo-immersive surveillance may lead to digital shaming campaigns against individuals perceived to have been violating some particular social norm when captured in an image. I attempted to explain why online communities seek to enforce norms against individuals who are not only not part of that online community, but also frequently do not even reside in their offline communities; I suggested it was likely a form of esteem competition. I also suggested that the online disinhibition effect explains why online sanctions may frequently appear disproportionate to the alleged infraction, and provided examples of some notable shaming campaigns. I went on to argue that the increasing deployment of geo-immersive technologies, thanks to the relative opacity of their operation, will make it difficult for individuals to accurately gauge the risk of whether their activities in public may be captured and distributed to a large anonymous crowd, thereby opening them up to ridicule, harm to reputation, or violence. I suggested that this poses a social-norms risk best understood as two-fold. First, individuals may be led to operate as though they are constantly under surveillance and will alter their actions in order to minimize risk; this is the initial

346 Steeves, supra note 340 at 207.
‘anticipatory conformity’, and I suggested that minority groups are likely to be those that suffer the most. Over time, as individuals repeatedly modify their behaviour in order to avoid this risk, I suggested that the opacity of the scrutiny may lead to those norms being internalized in a panoptic fashion. The result may then be that the conformity occurs not only in public space, but also behind closed doors. I then argued that this kind of norm internalization, even if initially affecting primarily minority groups, risks altering the character of public space itself, reducing it as a place of democratic debate and interaction. If this were to occur, then society as a whole may suffer from a less vibrant or robust public discourse.

**A Legal Response: When, and Against Whom?**

To reiterate, I am not arguing that limited deployment of geo-immersive technologies has already resulted in widespread majority norm internalization by minority groups or a neutering of the political vibrancy of the public square. I am not claiming that the existence of Google Street View has, single-handedly, significantly harmed minority groups or Canadian democracy in general. Rather, I am arguing that these harms may be the *unintended consequences* of unrestricted deployment of geo-immersive technologies in the future, as service providers compete to provide ever more detailed and frequently updated digital visual records of public areas. This justifies anticipatory regulation of systematic commercial surveillance of public spaces, rather than waiting to see if the harms I suggest may characterize widespread deployment of geo-immersive technologies do in fact arise. Privacy can be eroded gradually, so that it may not be noticed until it is ‘too late’; privacy is a culturally contingent experience, and what we demand as a reasonable level of privacy may vary over time. We may thereby become
attuned to ever-greater privacy violations without being consciously aware of it. The metaphor of the boiling frog captures this – if you throw a frog into a pot of boiling water, it will immediately jump out. But if you place the frog into a pot of cold water and gradually increase the heat, the frog will eventually be boiled alive. The social harms associated with surveillance and privacy loss can be interpreted in light of this metaphor – if the harms are diffuse and take time to build (as I suggest is the case with geo-immersive technologies), then we may not even realize we have allowed a system of surveillance to monitor us until it is already well established and accepted. As such, they provide ample reason for considering methods of lowering the probability that such consequences will occur and so the early years of geo-immersive technologies are critically important when it comes to striking the correct balance between corporate innovation and personal privacy. If I am correct that repeated exposure to an infrastructure of surveillance can lead to the internalization of certain social norms in a manner that is harmful, then the best way to prevent that internalization is to prevent the infrastructure from emerging in the first place. Transposed into a legal regime, then, this argues in favour of regulation that aims to prevent those harms from occurring;347 we should not wait for the harms to crystallize before taking action to prevent them. There are limits to this idea of ‘pre-emptive regulation’, though – laws that aimed to prevent every possible harm regardless of probability or magnitude would surely be stifling. In the context of geo-immersive surveillance, however, pre-emption is justified not only because of the growing body (if still relatively small in absolute

347 This may bear some resemblance to the ‘precautionary principle’, which “ensures that a substance or activity posing a threat to the environment is prevent from adversely affecting the environment, even if there is no conclusive scientific proof linking that particular substance or activity to environmental damage… its purpose is to encourage decision makers to consider the likely harmful effects of their activities on the environment before they pursue those activities.” See James Cameron & Juli Abouchar, "The Precautionary Principle: A Fundamental Principle of Law and Policy for the Protection of the Global Environment" (1991) 14(1) BC Int'l & Comp L Rev 1 at 1.
terms) of evidence I have described, but also because of the possibility of norm internalization – ex post facto regulation may simply be an inadequate remedy.

In Chapters 6 and 7, then, I will therefore consider the ways in which the law might respond to the risks I have outlined in this Chapter, as a means of pre-empting the social harms I have identified. In that regard, this thesis is also focused only on the utility of the relevant legal tools to be used against the commercial service provider, rather than the end viewers of the image, who may lead the campaigns of harassment against those caught in the images. This is for at least four reasons. First, the criminal law would seem to be an unsuitable vehicle for controlling the actions of the end viewers, since it is not at all clear that an individual using geo-immersive imagery could be charged with criminal harassment under existing ‘stalking’ legislation, simply for sharing or commenting on an image of someone. For instance, under the Criminal Code,

“No person shall … engage in conduct referred to in subsection (2) that causes that other person reasonably… to fear for their safety. (2) The conduct… consists of … (c) besetting or watching the dwelling-house, or place where the other person, or anyone known to them, resides, works, carries on business or happens to be.”

It seems improbable that the ‘watching’ of an individual through geo-immersive technologies could qualify under (c) of the above provision.

A more plausible technique for legally regulating the activities of the end viewers would therefore be in tort, but would also be both be difficult to accomplish and questionable in effect. To the extent that the ‘shaming’ is merely identification of the individual in the image and sharing of that image, then the secondary infrastructure of surveillance may be able to rely on

348 Criminal Code, RSC 1985, c C-46, s 264(1).
constitutionally protected expression rights for much of their activity. While it is true that rights under the *Canadian Charter of Rights & Freedoms*\textsuperscript{349} cannot ground private actions as between citizens, the Supreme Court has also held that the common law ought to be interpreted in a manner consistent with those rights.\textsuperscript{350} As Austin has argued, if a claim to privacy is based on the risks of “social pressure that promotes a kind of social conformity… then it is difficult to justify legal coercion to vindicate this interest unless it causes some kind of injury”, without running into counterbalancing freedom of expression concerns.\textsuperscript{351} In contrast, regulating the methods used in initial *collection* (as distinct from subsequent distribution) of imagery likely does not implicate the same constitutional concerns. This suggests an advantage to targeting the providers.

As I have noted in this Chapter, often times the identity of those conducting the campaigns may be difficult to discern. It *is* possible to bring an action revealing the identity of an anonymous Internet user in Canada,\textsuperscript{352} even if the plaintiff wishes to remain anonymous at the same time.\textsuperscript{353} However, there is no reason to assume that defendants would necessarily be Canadian; as I have indicated, once an image goes ‘viral’, it can become globally known. While none of these factors are absolutely fatal to a successful legal action, they do suggest that successfully pursuing such claims will be difficult, and for many, therefore perhaps out of reach. This also

\textsuperscript{349} *The Canadian Charter of Rights & Freedoms*, Part 1 of the *Constitution Act, 1982*, being Schedule B to the Canada Act (UK), 1982, c 11 (‘the Charter’)
\textsuperscript{350} See *Hill v Church of Scientology*, [1995] 2 SCR 1130 at para 91.
\textsuperscript{351} Austin, *supra* note 37 (‘Privacy & Private Law’) at 26.
\textsuperscript{352} See for instance *Warman v Fournier*, 2010 ONSC 2126.
\textsuperscript{353} See for instance *AB v Bragg*, 2012 SCC 46.
suggests an advantage to targeting providers over viewers— is almost always\textsuperscript{354} clear who has taken the image in the context of geo-immersive surveillance, because it is subsequently published. Moreover, even if a successful civil action (for harassment, perhaps) could be brought against an individual who had led or participated in a social shaming campaign against an individual captured in an image, this would not prevent those broader social harms from occurring unless a successful action could be mounted in almost every instance.

The third broad justification for targeting the service providers rather than end viewers is that the systems I have identified as currently exemplifying the first level of geo-immersive surveillance—the widespread generation and publishing of public imagery in an accessible online archive—are commercial in nature, currently requiring the resources of large corporations to fund and operate. The power of the end users in the bifurcated surveillance infrastructure that characterizes geo-immersive surveillance is dependent on access to this first level—limit the amount of imagery to which they have access or improve the techniques used to prevent identification of individuals in it, and you greatly limit the extent to which it can be used as a tool of behaviour modification. This does not mean there are no other forms of non-commercial “peer-to-peer” surveillance that might also lead to social shaming—indeed, I cite several examples of such activities in this thesis as evidence of the potential power of an anonymous audience. However, currently such peer-to-peer surveillance lacks the systemic component that characterizes its geo-immersive counterpart when it comes to the monitoring of

\footnote{The one exception to this may be if an image is taken from an geo-immersive website and then edited so as to remove any identifying ‘watermarks’ or logos, and then subsequently re-shared.}
For instance, while a significant amount of imagery is shared on online social networks, comparatively little of it is in the form of the surreptitious imaging of individuals in public space. The comparatively rare and irregular photography that characterizes such peer-to-peer surveillance and currently characterizes geo-immersive technologies is not likely to create the widespread norm internalization I suggest may accompany more widespread, systemic surveillance programmes. The harms I discuss in this thesis are dependent upon the evolution of geo-immersive technologies into a systemic tool; again, I do not claim that the existing systems have already radically altered the development or transmission of social norms in the areas they have imaged.

I will later argue that if restrictions can be placed upon the frequency of image collection, the more serious and widespread social harms I consider in this thesis may be avoided. Such restrictions only have relevance to the commercial providers, not the end users, because in the context of geo-immersive surveillance as defined in this thesis, only the commercial providers are collecting the imagery. In this sense, the bifurcation of the surveillance infrastructure actually can aid in regulatory efforts – by significantly restricting the initial collection undertaken by the commercial gathering infrastructure, I suggest that the surveillance-style harms identified in this Chapter can be prevented from arising. I later conclude therefore that despite the criticisms of surveillance scholars who argue that privacy law as exemplified by data

---

355 The recent announcement of Google’s “Glass” programme may change this, however, supra note 184. Some have raised concerns about the potential privacy impact of hundreds of thousands of individuals roaming the streets whilst continually recording. While such recording is of course possible with modern smartphones or small video cameras, the fears appear to be grounded in the inability of others to determine when “Glass” is or is not recording, since it is permanently worn; see for instance “US Politicians Quiz Google on Glass Privacy”, BBC News, online, http://www.bbc.co.uk/news/technology-22567061, last accessed May 17, 2013.
protection legislation cannot be antidote to surveillance, when the surveillance infrastructure is bifurcated between a commercial gathering entity and a non-commercial viewing entity, these criticisms have less salience. Furthermore, because PIPEDA is designed to balance off commercial interests with personal privacy, it already contains the mechanisms by which regulation can occur; this is easier than attempting to craft a regulatory regime through ad hoc actions after the claimed harm has already occurred. It is also more efficient – comparatively small changes in the regulations (or their application) now may have wide-ranging impacts in the future. Again, the goal is to restrict the growth of geo-immersive technologies in order to limit the possibility for broad social harms to arise, whilst still ensuring that service providers can develop and improve upon innovative technologies that have proved popular with many Canadians.

In sum, these are all reasons that suggest the most appropriate method of legal regulation is to focus on the behaviour of the commercial service providers, and I will expand upon this discussion in Chapters 6 and 7. However, in the next chapter I want to return to the connection between autonomy and privacy that I touched upon in Chapter 1, because it helps explain some of the flaws that I will later suggest characterize the way the law in Canada is currently responding to the use of geo-immersive technologies.
Chapter 5: Rethinking Autonomy & Privacy

I argued in the last two chapters that heavy deployment of geo-immersive technologies ought to ultimately be seen as a form of public surveillance that, if left unchecked or unregulated, may bring with it some serious social consequences. I have also suggested that this form of surveillance is best understood as a problem related to privacy, because it forces individuals in public to subject themselves to an unpredictable and unwanted gaze, far removed from their actual location. Because they cannot accurately predict when or where they will be observed, or who will be doing the observing, I have argued that this kind of gaze is fundamentally different than the kind of gaze one typically may be subject to simply by virtue of being in public places. But the dominant liberal ‘privacy as withdrawal’ or ‘privacy as a zone of freedom’ theories that I outlined in Chapter 1 have a hard time grappling with privacy claims made in public places because in such cases the individual has clearly relinquished any desire to withdraw – when in public, they are actively choosing to be amongst others. This is problematic because, as I will show in later chapters, such approaches dominate much of the legal approach to privacy claims.

I want to argue that privacy claims in public can be better understood if we abandon the kinds of barrier metaphors that characterize ‘withdrawal’ approaches to privacy, and instead think of privacy in relational terms. In this chapter, then, I first consider existing critiques of boundary approaches to privacy, and then suggest that a dialectical approach to privacy is the best model for considering ‘privacy in public’ interests. It is predicated on not understanding privacy as a state of withdrawal, but rather upon the ability of the individual to adequately negotiate their relationship with the community across a variety of levels. I then attempt to connect that
interpretation of privacy to a normative underpinning of ‘relational autonomy’, drawn from the work of a number of feminist legal scholars. This ‘relational’ approach to privacy, I suggest, can best explain the kind of privacy interests that are at stake in the context of geo-immersive surveillance, and indicates that they extend beyond those who are actually recorded in an image to those living in a society characterized by regular, systematic digital photography of public space for commercial purposes.

Reinterpreting the Metaphor of the Boundary: From Spatial to Dialectic Accounts

As I noted in Chapter 1, there are many scholars who reject boundary approaches to privacy dependant on a relatively strict public/private dichotomy or relatively fixed spatial boundary. Various conceptions of privacy have acknowledged that there must be some level of fluidity as individuals transition between public and private areas of their life, and that the two areas often overlap, rather than exist as separate ‘locked boxes’. In this section I want to consider conceptions of privacy that acknowledge this fluidity. I suggest however that they may still struggle to account for privacy claims in the context of geo-immersive surveillance if they are not also tied to an underlying conception of autonomy that recognizes the importance of social context in the protection of capacities for its advancement; in other words, I seek to ultimately infuse privacy with the lessens of relational autonomy.

Schwartz, for instance, rejects the dominant liberal paradigm, concurring with Post’s claim\textsuperscript{356} that privacy does not function only as a barrier for individuals against the community, but also

creates rules that constitute both the individual and the community.\(^{357}\) This emphasis on both the individual and the community leads both to define privacy on a functional basis, suggesting that privacy ought to be seen as creating ‘information territories’ that are multi-dimensional insofar as information shifts in and out of them, depending on the context.\(^{358}\) Importantly, these territories rise and fall in order to both help the individual as an individual and to define their terms of social interaction within the community.\(^{359}\) This view of privacy then is connected not only to the protection of the interests of the individual, but also of society more generally, since the ways in which information territories shift will alter patterns of knowledge, and will have the capacity to stimulate or discourage social expression and action.\(^{360}\) It is this capacity, says Schwartz, which gives privacy its constitutive function in society; it must therefore be seen as more than a right to individual control, for such a conception is “incapable of generating the kinds of public, quasi-public, and private spaces necessary for effective democratic self-rule.”\(^{361}\)

Austin argues that an account of privacy based upon the ability to present oneself to others need not depend on determining different spheres of public and private life. She suggests that our interest in privacy is not only a claim to be protected from social pressure that results from a particular self-presentation, but rather is about “protecting the conditions for self-presentation.”\(^{362}\) This self-presentation, she says, is an act of “social communication”, and surveillance disrupts this communication by denying us the knowledge of who our audience

\(^{358}\) Ibid.  
\(^{359}\) Ibid & Post, supra note 356 at 985.  
\(^{360}\) Paul M Schwartz, "Internet Privacy and the State" (1999) 32 Conn L Rev 815 at 834.  
\(^{361}\) Schwartz, supra note 357 at 1660.  
\(^{362}\) Austin, supra note 37 (‘Privacy & Private Law’) at 36.
When we do not know to whom we are presenting ourselves, Austin contends, self-presentation cannot actually be effective. However, she also argues that violations of ‘privacy as identity’ in this fashion will “only occur when the dissemination of private information also undermines one’s capacity for self-presentation.” Such capacity is undermined, according to Austin, when we are forced to incorporate into our self-presentation this previously private information; “the salient distinction is not between public and private spheres of life, but rather between the types of audiences” to whom we were presenting.

Applied in the context of geo-immersive surveillance, this would appear a useful means of explaining how individuals might retain certain kinds of privacy interests whilst in public space – the bifurcated surveillance infrastructure of which I have spoken is premised on disseminating information to an entirely new audience, unknown to the subject of the photograph. As Austin says, “changing the identity of one’s audience through surreptitious surveillance or unexpected publication” can be understood as a privacy violation. A widespread system of geo-immersive surveillance would do just this – as I earlier argued, it would disrupt the ability of individuals to make an informed calculation about their exposure to audiences when in public.

Nissenbaum also believes that a reliance upon a strict public/private boundary results in an approach to privacy that is unable to sufficiently account for many of the privacy losses that may be caused by the increasing digitization of all areas of life. While the focus of this thesis is more narrowly focused on a particular kind of public surveillance undertaken by a particular

---

363 Ibid.
364 Ibid.
365 Ibid.
366 Ibid.
367 Helen Nissenbaum, “Privacy as Contextual Integrity” (2004) 79 Wash L Rev 119 at 120.
kind of entity and done so in a particular way, it is unquestionably tied to the same digital transformation of modern life in which Nissenbaum is interested. She argues that conceptions of privacy based on non-interference or control cannot account for many of the issues raised by modern types of ‘public’ surveillance in part because of their reliance on public/private dichotomies.\footnote{Ibid.} She advocates, instead, for an account of privacy that is characterized by fluidity rather than rigidity between the realms of ‘public’ and ‘private’; she terms it ‘privacy as contextual integrity’, based on the premise that all aspects of our lives are governed by some kind of information flow. Nissenbaum observes that as individuals go about their lives, they are constantly shifting between differing ‘realms’ that can be thought of as either \textit{locational} (workplace, home, church, the street, etc.), \textit{social} (friends, co-workers, family, strangers, etc.), or \textit{action-related} (working, seeking medical care, voting, shopping, etc.).\footnote{Ibid.} Each of these realms “involves, indeed may even be defined by, a distinct set of norms, which governs its various aspects such as roles, expectations, actions, and practices.”\footnote{Ibid.} Nissenbaum argues that the flow of information between these realms is typically governed by ‘norms of appropriateness’ and ‘norms of distribution’; when either norm is breached, we ought to see it as violation of contextual integrity, and thus, privacy.\footnote{Ibid.}

She suggests that norms of appropriateness “dictate what information about persons is appropriate… to reveal in a particular context”,\footnote{Ibid.} thus addressing the difficulty of a dichotomy between private and non-private information. Since the norm of appropriateness is inherently
contextual, information can be tagged as private in certain contexts, and non-private in others, rather than being permanently tagged as one or the other. In the context of geo-immersive surveillance, such an approach to privacy could theoretically explain why being viewed by passers-by on a public street is not a loss of privacy that ought to be actionable, but why the widespread distribution and public archiving of records of those movements should be. Under this approach, even ‘public’ matters might generate a privacy claim if they inappropriately breach the ‘norms of distribution’ (those that govern the transfer or flow of information from one party to another).\footnote{Ibid.} What matters, therefore, is not “whether [the] information is appropriate or inappropriate for a given context, but whether its distribution, or flow, respects contextual norms of information flow” \cite{contextual, non-private}.

The aforementioned approaches appear, however, to be dependent on the dissemination of information (‘contrary to the norm of distribution’, for Nissenbaum; ‘in a fashion that undermines one’s capacity for self-presentation’, for Austin). This means that while they are useful ways of explaining why surveillance should be felt as a privacy loss for those imaged, the necessity of dissemination in these theories appears to struggle to explain how individuals not actually subject to public street surveillance could be described as suffering a privacy loss, since their information is not actually disseminated if it is not captured in the first place. Altman’s approach, in contrast, appears to focus more on the ability of the individual to regulate the potential for contact and therefore does not appear as dependent on the need for information dissemination. His proposition is that “privacy is an interpersonal boundary process by which a

\footnote{373 Ibid.}  
\footnote{374 Ibid.}
person regulates interaction with others.” Like Schwartz, then, Altman sees privacy as something that allows a negotiated level of exposure by an individual to the community. Although his ideas are therefore based on a boundary, it is not the same type of boundary upon which withdrawal approaches are based; it is as “a dynamic process involving self-control over a self-boundary.” Privacy understood in this manner for the individual is not just therefore a claim for a protected interest over a certain area or thing, but is rather a power of “boundary regulation” in which the individual has an on-going ability to negotiate where the boundary ought to lay. Under the conventional liberal approaches, privacy is binary – once you have allowed intrusion into your personal zone, or allowed access to yourself, or relinquished control over your information, then typically claims to privacy based on such conceptions necessarily fail – you no longer have a ‘reasonable expectation of privacy’. Critically, this need not be the case with a dialectical understanding of privacy, which instead suggests that privacy “involves a synthesis of being in contact with others and being out of contact with others… [since] the desire for social interaction or non-interaction changes over time and with different circumstances.” Importantly then, this view of privacy is not only about regulating the flow of information, but also about regulating relationships; it is a “dialectic process, which involves both a restriction of interaction and a seeking of interaction” (emphasis mine). As Steeves


376 Altman, supra note 375 at 6.

377 Ibid.

378 Ibid.

379 Ibid.
argues in her consideration of Altman’s work, “privacy is the boundary between the self and the other that is negotiated through discursive interaction between two or more social actors.”

This is therefore a useful way of understanding privacy interests in the context of geo-immersive surveillance of public space. The dialectic approach accepts that by entering into a public area individuals seek (or at least accept) some level of interaction with those around them and therefore have no claim to visual privacy vis-à-vis those others. Simultaneously, however, it recognizes that they are not seeking such interaction with anonymous groups far removed from that scene, spatially and temporally, and therefore cannot be said to have relinquished their privacy rights versus that group, unless there is evidence to the contrary. Moreover, as Altman argues, “it is not the exclusion or inclusion that is vital to self-definition, it is the ability to regulate contact when desired... [it is] when the permeability of those boundaries is under the control of a person” that both self-development and autonomy are served. This means that to the extent the existence of a surveillance infrastructure threatens to hamper that ability – which I have argued is precisely the case with the irregular or unpredictable capture of imagery by geo-immersive technologies – then that infrastructure can be interpreted as causing a privacy loss, even absent actual collection and subsequent distribution/dissemination of imagery. It is a privacy loss because the ability of the individual to control their exposure to an audience removed temporally and spatially is interfered with.

380 Steeves, supra note 340 at 206.
381 Altman, supra note 375 at 50.
Steeves also advocates an understanding of privacy as “a dynamic process that is exhibited by the individual in social interaction with others, as the individual withdraws from others into solitude or moves from solitude to intimacy and general social interaction.”\(^{382}\) In this manner, Steeves recognizes that a shift away from solitude is not necessarily a shift away from privacy; “privacy is no longer juxtaposed against social interaction… but is a potentiality throughout the full range of human experience.”\(^{383}\) Palen & Dourish offer an account that directly builds upon Altman’s work, but that reinforces the concept that ‘the negotiated boundary’ is not the same as the boundary that is typically associated with the individualistic approaches to privacy that I have criticized. That is, it is not simply a wall marking the difference between what is private and what is public. They suggest that there are at least *three* different kinds of boundaries that are relevant to a privacy discussion, none of which share the same public/private distinction common to the individualistic conceptions – the disclosure boundary, the identity boundary, and the temporality boundary.\(^{384}\) The disclosure boundary lies, essentially, at the interface between one’s personal life and public face. Unlike a conventional public/private boundary, this is not only about the power to withdraw, but rather about engagement. For example, maintaining a state of privacy may actually “require disclosure of personal information or whereabouts… we all have thoughts or facts we would like to keep secret, but most of us also need to ensure that others know something about ourselves, for personal or professional reasons” (emphasis in original).\(^{385}\) Palen & Dourish note though that revealing information for such reasons may also be done, paradoxically, to decrease our accessibility (they use the example of academics who

\(^{382}\) Steeves, *supra* note 340 at 206.

\(^{383}\) Ibid.

\(^{384}\) Palen & Dourish, *supra* note 375 at 131.

\(^{385}\) Ibid.
maintain web pages with curricula vitae and downloadable copies of published papers, etc. as way of both advertising their professional status but also as a means of reducing the need for personal contact to obtain such information. This recognition that the disclosure boundary can be used as a way of simultaneously lowering privacy through increasing visibility/publicity whilst decreasing accessibility (and thus, in a sense, increasing privacy) is an important point. In the context of this thesis, it might suggest that sometimes we seek social contact in public space in order that we may avoid it in others. People may choose to prefer to meet at a restaurant rather than inviting someone over for dinner, for instance – this choice to meet in a public place may well be done to maintain the privacy of the home for instance. Indeed, in many cultures “dinner parties” at a private residence are rare, for this very reason. As Palen & Dourish note, “active participation in the networked world requires disclosure of information simply to be a part of it… [but] problems emerge when participation is not deliberate.” I would argue that this principle extends beyond the informational realm and into the physical – participation in public space requires some associated disclosure of information to those immediately present, but geo-immersive surveillance forces are far greater level of than is actually necessary for typical participation. For those unwilling to be a part of the surveillance project then, participation in that widespread disclosure is surely not deliberate.

Palen & Dourish’s ‘identity boundary’ lies at the intersection of self and other. Traditional approaches seek to keep out the other, protecting the self from harm, but they argue this fails to take into account that people not only act as individuals, but also as members of

386 Ibid.
387 Of course, as noted in Chapter 2 there are those who have sought out the cameras for the purposes of performance art, but they appear to thus far be relatively few in number.
social/cultural/professional groups; when they act in the latter manner, they must adhere to certain expectations, and those expectations often have particular requirements related to privacy, such as client confidentiality for lawyers.\textsuperscript{388} Thus, a conception of privacy that sets up the idea of the individual as something separate from the group is necessarily inadequate; our identities are built, at least partially, in conjunction with our affiliations and allegiances. What is more, just as the “self” is a contextual construct, so too is the “other” – one’s interactions with professional colleagues are different than those with those with fellow riders of public transit.\textsuperscript{389} Again, the dialectical approach suggests that I might willingly disclose (or even be required to disclose) many things about myself within a professional context in order to create or maintain a particular ‘identity’, whilst at the same time shielding that identity from other groups. The power to regulate these boundaries is threatened by commercial public surveillance because it can remove our ability to develop and present different identities according to context; this is consistent with Austin’s argument, supra. Palen & Dourish argue that our ability to accurately perceive others is compromised in the digital world because “rather than interact directly with another person, we… make assessments from a representation that acts in proxy”, and in digital environments “that representation [is] often impoverished.”\textsuperscript{390} The same is true for geo-immersive surveillance imagery, which is often highly reductive in nature, and yet can still be the basis for anonymous groups seeking to ascribe motivations to those shown within them. This is further complicated by what Palen & Dourish term ‘information persistence’ which, they argue, “further complicates regulation of the self/non-self boundary.”\textsuperscript{391} Information persistence

\textsuperscript{388} Palen & Dourish, supra note 375 at 132.
\textsuperscript{389} Ibid.
\textsuperscript{390} Ibid.
\textsuperscript{391} Ibid.
is a key characteristic of many digital interactions, and as I have indicated, the possibility of viral spread of imagery – making it effectively untouchable by takedown requests – means it also characterizes geo-immersive surveillance. While in certain cases individuals may intentionally construct identities by taking advantage of this digital permanence (think of individuals selecting exactly which personal information to display to their acquaintances in an accessible form on digital social networks), “we have very little control over representation of ourselves that are artefacts of simply having been somewhere or done something at a particular time.” This is the case, of course, when geo-immersive imagery being captured and widely distributed without prior knowledge by the subject of the image.

The third boundary Palen & Dourish identify is the temporal boundary, which is the location of the tension between past, present, and future. Their premise is that “specific instances of information disclosure are not isolated from each other; they occur as the outcome of a sequence of historical actions, and as the first of many expected actions stretching out into the future.” Privacy management, therefore, must take into account this backdrop. The temporal boundary is dialectical because while sometimes individuals may respond in the present based upon disclosures that have been made in the past, “patterns, conventions, and genres of disclosure… are [also] made to be broken; conventions can be invoked by breaching as well as following them.” The conversion of previously ephemeral activities that were only viewable (and quickly forgotten) by those immediately present into archived records of the same activities is, of course, one of the key features of geo-immersive surveillance. Understanding privacy as a

392 Ibid.
393 Ibid.
394 Ibid.
dialectical process that involves this temporal tension helps to explain why the archiving of activities we nonetheless undertook in full view of the ‘public’ ought to attract some kind of privacy interest.

Considering privacy as a means of the individual negotiating their relationship with the community in such a dialectical fashion offers the best account of why commercial surveillance of public spaces through geo-immersive technologies ought to be seen as implicating important privacy interests. A claim to privacy as a claim to control the boundary of disclosure related to protection of both a private life and a public face, the boundary of identity related to development of the self and interaction with the community, and the boundary of time related to the disclosure of information and the ways it can be used for decision-making at points in time separate from its initial disclosure together can form a basis for saying that certain geo-immersive practices intrude upon or weaken personal privacy. That is, public surveillance that significantly disrupts one or all of those boundaries ought to be seen as a significant privacy loss, including for those who are not photographed directly – what matters is the way in which our ability to control our exposure is altered, in an unpredictable fashion. The existence of the infrastructure of surveillance, operating irregularly disrupts our ability to adequately be able to negotiate our desired levels of exposure, whether or not we are personally recorded in an image.

Transforming these ideas into statements about when a privacy claim ought to be granted by the law requires, of course, a connection to underpinning values. The reliance of Nissenbaum’s ‘contextual integrity’ approach, for instance, on existing ‘norms’ tends to create a presumption
in favour of the status quo, and this could be problematic if entrenched standards of either appropriateness or distribution are not necessarily robust enough to protect against some of the modern privacy threats.\textsuperscript{395} Grounding a legal framework aimed at regulating commercialized public surveillance in a theory of privacy as contextual integrity might only be effective if there are particular norms already in effect that support particular goals; contextual integrity, being tied to practice and convention, may not alone have sufficient “prescriptive value or moral authority.”\textsuperscript{396} In the context of geo-immersive surveillance then, as people become ‘used to’ having their public movements or activities monitored by anonymous audiences, reliance on a contextual integrity approach might fail to offer any meaningful protections. On the other hand, there is also the opposite risk that her theory might be overly conservative, if it saw privacy violations in \textit{any} new technological means of managing personal information, simply because it was new (and therefore a break in an existing norm of distribution).\textsuperscript{397} Schwartz also places reliance on largely unstated ‘norms’ – he argues for lines between public and private to be drawn and redrawn along different coordinates in order to reflect “different informational privacy norms”.\textsuperscript{398} Again, without knowing the content of these norms, it is difficult to know if Schwartz’s conception will leave us with a relatively robust or relatively weak defence of privacy interests. Schwartz seems to argue for a general framework tied to the interests of the democratic community – public accountability requires access to personal information, and bureaucratic rationality needs it in order to allow administrative structures to function.\textsuperscript{399} But this fails to explain when claims to privacy in public spaces ought to be recognized, though

\begin{footnotesize}
\begin{enumerate}
\item[395] Nissenbaum, \textit{supra} note 367 at 143.
\item[396] \textit{Ibid}.
\item[397] \textit{Ibid}.
\item[398] Schwartz, \textit{supra} note 360 at 834.
\item[399] \textit{Ibid}.
\end{enumerate}
\end{footnotesize}
logically his implication might be that such recognition could be justified where it would prevent harm to (or work to protect) general democratic interests. While I have argued, that geo-immersive surveillance might result in such risks, it would not seem to account for many of the more personal harms as well. The focus on shifting points of access and the need to create an interface between public and private aspects of life in the dialectical approaches is welcome, but without a normative underpinning it cannot tell us which transgressions of that interface ought to ground legal complaints and which should not. My suggestion is, then, that without the connection to a ‘relational autonomy’, even conceptions of privacy that accept that there is no dichotomous split between things that are public and things that are private may not necessarily provide suitable grounding for a legal privacy regime that is responsive to public surveillance issues. It is that idea that I now turn.

**Relational Autonomy**

The individualistic account of autonomy sketched in Chapter 1 has come under sustained criticism from both those who reject the liberal conception of the individual and its associated connection to autonomy entirely, and those who wish to reconstruct it. In this section, I wish to consider the arguments of those who have sought to do the latter. Since I believe there is an important linkage between accounts of autonomy and conceptions of privacy, these reconstructed accounts might better inform theories of privacy in a fashion that does not overly privilege spatial questions. From there, it is then easier to imagine how a set of legal tools might

---

be developed to better respond to the issues I have raised in this thesis regarding the deployment of geo-immersive technologies as a means of conducting public street surveillance.

Despite the obvious connection between liberal theory and the individualistic account of autonomy, there is nothing about approaching autonomy in a manner that is not starkly individualistic that is inherently “anti-liberal” or demands the wholesale rejection of its key tenets – indeed, there are numerous liberal approaches to autonomy that recognize that “an autonomous personality can only develop and flourish against a background of biological and social constraints.” Raz, for instance, recognizes that “the completely autonomous person is an impossibility,” while Dworkin admits “substantive independence… would make autonomy inconsistent with loyalty, commitment, benevolence, and love, all of which are important values.” Crittenden too has long advocated for liberals to “jettison from their theories any remnants of atomistic individualism”, but also “resist the association of autonomy with communal boundaries” that he sees as the defining element of the communitarian approaches.

The need is not, then, to entirely abandon the liberal account of autonomy, but rather to enhance it, to “reformulate [it]… without buying into the negatives of liberal legalism.”

There is a distinction, however, between those liberal accounts that reject an atomistic approach to autonomy and those that argue that protecting autonomy in fact requires active protection of

---

401 Raz, supra note 20 at 155.
402 Ibid.
403 Dworkin, supra note 15 at 21.
404 Crittenden, supra note 27 at 37.
certain social contexts. The reformulation I wish to consider here – relational autonomy – is of the latter type, and is perhaps best associated with the work of Nedelsky. Drawing from the work of feminist theorists who found the individualistic approach to autonomy inconsistent with the aspirations of feminism, Nedelsky seeks not to abandon the value of autonomy entirely, but rather to improve our understanding of the ways in which it can be nurtured and protected. A number of feminist scholars have argued that the individualist approach to autonomy privileges it as a value for men. Friedman, for instance, argues it is “antithetical to women’s interests because it prompts men to desert the social relationships on which many women depend for… their well being [and that of] their children.” Benhabib suggests that the “[liberal] tradition, when it considers the autonomous individual… implicitly defines [it] as the standpoint of men.” Griffiths too argues that liberal ideas of autonomy are based upon the “unencumbered man… free of ties”, whereas women “assert value… in [a] social life which is rooted in ties to the family, friends, neighbourhood, culture, and family history.” Barclay also sees the typical liberal conception of the autonomy as “starkly at odds with many women’s experiences.” Likewise, Code believes that a focus on autonomy that places the importance of free action above all else privileges the interest of men, who are not expected to undertake the same social roles as women.

406 See Nedelsky, supra note 46; Nedelsky, supra note 52.
407 Friedman, supra note 31 at 36.
to “retain [autonomy’s] basic value… [while rejecting] its liberal incarnation.”  She still accepts, for instance, that “to become autonomous is to come to be able to find and live in accordance with one’s own law.”  The relational account does not disagree that autonomy is the ability to be self-governing, nor that it is valuable – what is disputed is that it is freedom from external influence that enables autonomy.

Relational views underscore the social embeddedness of selves while not forsaking the basic value commitments of liberal justice. They underscore the social components of our self-concepts as well as emphasize the role that background social dynamics and power structures play in the enjoyment and development of autonomy.

The relational accounts are therefore not seeking to redefine what autonomy is so much as redefining how it can be achieved, and are consequently focused on whether the individuals in fact have the substantive capacities for that autonomy. The central proposition is that the substantive capacity for autonomous decision-making can only come when one is embedded in the right kinds of social environments. In Friedman’s words, “persons [are] fundamentally social beings who develop competency for autonomy through social interaction with other persons.”

Kupfer argues, for instance, that while the stranded sailor on an island is ‘perfectly autonomous’ under an individualist account, lacking any external restrictions other than the natural world, this misses the point: “without the opportunity to be with others, autonomy is empty.” Individualistic accounts, says Nedelsky, “[miss] the reality that the capacity for autonomy can only develop and thrive when fostered by constructive relationships, such as

---

412 Nedelsky, supra note 46 at 7.
413 Nedelsky, supra note 52 at 123.
415 Friedman, supra note 31 at 41.
416 Kupfer, supra note 405 at 159.
those with parents, teachers, friends, and agents of the state.\textsuperscript{417} Thus, she argues, eliminating external restraints is no guarantee of autonomy, since one requires “relationships that provide the support and guidance necessary” for its development.\textsuperscript{418} Under the relational accounts, the capacity of the individual for autonomous decision-making is not \textit{automatically} threatened by the relationships it has with ‘the collective’; quite to the contrary, those relationships may at times be vital for that autonomy. Thus, “the collective is not a ‘threat’ to individuals, [but] is constitutive of them.”\textsuperscript{419}

For Nedelsky, the very idea of exercising autonomy as an isolated figure is a misnomer, as “the content of one’s own law is comprehensible only with reference to shared social norms, values, and concepts.”\textsuperscript{420} Autonomy, she says, “can thrive or whither in adults depending on the structures of relationships they are embedded in.”\textsuperscript{421} Thus, per Stoljar, the most autonomous individuals are \textit{not} in fact those who are most isolated; instead, autonomy is \textit{also} a characteristic of “agents who are emotional, embedded, desiring, creative, and feeling.”\textsuperscript{422} Nedelsky seeks to replace an understanding of autonomy that focuses on exclusion and the dichotomy between the individual and the collective with one based on the metaphor of ‘childrearing’, built on the idea that children are not simply born ‘autonomous’ any more than they are born ‘adult’. Children do not pass into adulthood simply by virtue of eliminating familial bonds, Nedelsky argues, but rather grow into autonomous adults as a result of being raised in an appropriate manner by a

\textsuperscript{417} Nedelsky, \textit{supra} note 52 at 167.
\textsuperscript{418} Nedelsky, \textit{supra} note 46 at 12.
\textsuperscript{419} \textit{Ibid}.
\textsuperscript{420} \textit{Ibid}.
\textsuperscript{421} \textit{Ibid}.
loving family or community, in which bonds and relationships remain an important vehicle through which autonomy can be expressed. Modell notes, for instance, that “the child’s creative use of solitude requires the presence of the mother in order to affirm the continuity of the self. The private self... frees one from dependency, yet requires the Other for its continued existence.”

Thus, advocating a relational approach to autonomy does not deny that the ‘self’ is an important construct, but rather argues that it is meaningless without reference to social context, and thus one cannot legitimately protect the ‘autonomous self’ simply through the elimination of external influences. As Tice and Baumeister argue, “relating to others is part of what the self is for. The self is constructed, used, altered, and maintained as a way of connecting the individual” to others (emphasis in original). Kupfer, then, concludes that “autonomy derives its meaning from a social context in which we exercise [it] in relation to others, as social beings.”

The core tenet of relational accounts, then, is that autonomy can only be properly achieved “under socially supportive conditions.” Developing the capacity for autonomy or ensuring its continued exercise requires not simply guarding against certain kinds of overt coercive external restrictions upon individuals, but also the protection of social contexts that assist in our capacity for autonomous thinking and action. The “autonomy-undermining injustices” to which individuals are constantly vulnerable are not only the kinds of external interferences against

---

426 Anderson & Honneth, *supra* note 11 at 130.
427 Nedelsky, *supra* note 52 at 55.
which the individualist conception of autonomy might guard, but also, as Anderson and Honneth note, disruptions to social relationships generally.\textsuperscript{428} The importance of the social context also means that autonomy is something that can be gained and lost – as one’s social context shifts, so too might one’s capacities to engage in autonomous decision making and action. This means that the proper social context must continually be nourished, as “people’s capacities for autonomy will vary enormously both across individuals and within a given person across time and across different spheres of life.”\textsuperscript{429}

Of course, much as there are competing accounts of ‘liberal’ autonomy, so too is the case here; “relational autonomy does not refer to a single unified conception of autonomy, but rather is an umbrella term designating a range of related perspectives”, all of which are based on the idea that the social context in which an individual is embedded is vital for any realization of autonomy.\textsuperscript{430} There is, for instance, a robust debate regarding whether or not relational autonomy accounts ought to treat “relationality as conceptually necessary for autonomy, rather than just causally necessary.”\textsuperscript{431} In other words, are “agents intrinsically relational because their identities… are constituted by elements of the social context in which they are embedded” or are “agents causally relational because their natures are produced by certain historical and social

\textsuperscript{428} Anderson & Honneth, \textit{supra} note 11 at 130.
\textsuperscript{429} Nedelsky, \textit{supra} note 52 at 173.
\textsuperscript{430} Stoljar & Mackenzie \textit{supra} note at 4.
conditions”?

To say that relationality is conceptually or constitutively necessary would mean that an individual would need to be embedded in certain relationships to be considered autonomous; “social conditions are more than background conditions… and autonomy cannot be spelled out without direct reference to a person’s social environment.” However, since in either case the point is that social conditions are important and relevant to the achievement of autonomy, it is therefore unnecessary for the purposes of this thesis to advance once conception over another. What is important is the “shared conviction that persons are socially embedded and that [their] identities are formed within the context of social relationships.”

Accepting a relational component to autonomy does not require contending that all relationships are beneficial – indeed, many of the risks I see in public surveillance come from the existence of an over-zealous community. Thus, while, yes, the community can indeed be a “source” of rights for the individual, it still has the potential to be a threat. In this sense, the community is inherently Janus-faced; it can be both a hindrance and a help to the cause of autonomy. While autonomy may indeed be nurtured and protected though a supportive social context, there is no need to reify particular kinds of social relations at the expense of the ability of the individual to extricate themselves from damaging social contexts within which they may find themselves – including those that in other contexts may be supportive, such as family or intimate partners. As Mackenzie argues, while relationships are vital for autonomy, “social relationships that… do not

---

432 Stoljar & Mackenzie, supra note 422 at 22.
434 Stoljar & Mackenzie, supra note 422 at 4.
435 Nedelsky, supra note 46 at 21.
recognize our moral equality” can hamper it.\textsuperscript{436} She notes that capacities for autonomy are “vulnerable to our relationships with others in all the different spheres of our lives.”\textsuperscript{437} Her argument is that the “social character of autonomy” does not demand paternalistic interference to assure that individuals are autonomous, but rather “highlights the positive obligations of social institutions to promote the autonomy of citizens by fostering the social conditions for autonomy.”\textsuperscript{438} Nedelsky too accepts that a relational interpretation of autonomy “does not mean that people are determined by their relationships”, or that “all relationships are good”, and that autonomy must “allow people to extricate themselves from bad relationships.”\textsuperscript{439}

I seek to draw from this relational approach to autonomy, then, only the contention that generating and protecting capacities for the development and exercise of autonomy requires not merely the elimination of external influence, but rather the protection of a positive social context in which the individual is embedded. The argument is that a supportive social context is for most people necessary for the achievement and maintenance of autonomy, understood as self-governance. While this approach rejects an individualist approach that argues that eliminating external influences necessarily generates or protects the conditions of autonomy, it nonetheless remains alive to traditional liberal concerns regarding the harm that may befall individuals subject to an overbearing community. I argued in Chapter 1 that the approach one takes to autonomy frequently colours subsequent interpretations of privacy, and that an individualistic idea of autonomy tends to lead to barrier-based views of privacy. In the next section then, I

\textsuperscript{436} Mackenzie, supra note 431 at 524.
\textsuperscript{437} Ibid.
\textsuperscript{438} Ibid.
\textsuperscript{439} Nedelsky, supra note 52 at 32.
want to consider if the idea of relational autonomy as sketched above can underpin a different approach to privacy that is not dependent upon spatial questions or barrier metaphors.

**Relational Privacy**

Nedelsky has argued that in the context of *informational* privacy “the metaphor of a boundary is far less helpful than direct exploration of the relational dimension of how the circulation of information matters to people.” While she does not explore this idea in detail, the suggestion appears to be that it is not enough to protect privacy simply by shielding the individual from overt external influence, but rather that privacy can only be protected when the impact of information is taken into account, regardless of whether it is “sensitive” or “personal”. I would suggest also that the circulation of information has an impact beyond those to whom the information directly relates, and believe this can form the basis of what can be termed ‘relational privacy.’

I am not the first to describe an idea of ‘relational privacy’, though my conception differs somewhat from those that came before. Cohen, for instance, has described “relational privacy” as the “right to not have one’s constitutive identity needs violated or interfered with by the state or by third parties without very compelling reasons indeed.” She was writing this within the context of the American jurisprudence surrounding the abortion debate, and was therefore primarily concerned with protecting a woman’s zone of “decisional autonomy, inviolability of

---

personality, and a sense of control over one’s identity needs”. Thus, while she uses the term ‘relational privacy’, Cohen still appears to rely upon a conception of autonomy reliant primarily upon the boundary metaphor, seeking to prevent interference in a woman’s right to make decisions about her body. Grounded in US abortion rights debates, this is understandable – feminist theorists have argued that ‘privacy’ rights have long been used to subject women to domestic violence by creating a zone into which the state ought to not tread, whilst simultaneously advancing a belief that privacy (understood really as ‘decisional privacy’) is vital to the protection of abortion rights under the 14th Amendment. Cohen is not, then, arguing that relational privacy is necessary to protect particular social contexts that help create autonomy, but is instead arguing that relational privacy creates a zone of decisional autonomy that allows individuals to develop their identities in conjunction with others.

The idea that privacy can protect relationships is also not new, though in my view relational privacy is not entirely the same thing. Rachels, for instance, argues that privacy is important because it allows for a diversity of relationships. On his account, there is a close connection between our ability to control who has access to us and our ability to both create and maintain a variety of relationships. The ability to maintain an array of relationships on different levels with different kinds of people is, he says, “one of the most important reasons why we value privacy”. Schoeman also believes that in addition to protecting aspects of the self, supra, privacy also “marks out something morally significant… about what it is to have a close

442 Ibid.
443 See Roe v Wade, 410 US 113.
445 Ibid.
relationship with another [person].”\textsuperscript{446} He suggests that entrusting another individual with intimate information about ourselves is a means of conveying to that individual that the information is important to us. By respecting the decision regarding with whom to share these intimacies, we “enrich social and personal interaction by providing contexts for the development of varied kinds of relationships and multiple dimensions of personality.”\textsuperscript{447} Reiman, on the other hand, critiques this vision of privacy, suggesting that it improperly creates a market conception of intimacy by positing that levels of intimacy are determined by what we choose to withhold from others. There must be more, says Reiman, to intimate relationships than simply swapping information.\textsuperscript{448} I concur – intimate (and non-intimate) relationships are surely about more than simply choosing or declining to swap information, though at the same time it is possible to imagine that such relationships might be furthered or retarded by decisions related to the exclusive sharing of certain kinds of information between partners.

But accounts of privacy that suggest it has value in protecting relationships tend to still be based on boundary metaphors – in other words, that ‘private space’ is necessary to allow relationships to grow. Such approaches would seem to offer little protection against public surveillance, since it could be argued that intimate relationships thrive primarily behind closed doors. Relational privacy therefore suggests that privacy is not only about creating a ‘zone’ in which intimate (or other particular types of) relationships can grow; instead, it can be seen as reflective of the kind of dialectic approach I earlier outlined, married to a normative goal of protecting social contexts that assist in the development and maintenance of personal autonomy. The lessons drawn from

\textsuperscript{446} Schoeman, supra note 35 at 403.
\textsuperscript{447} Ibid.
\textsuperscript{448} Reiman, supra note 41 at 305.
relational accounts of autonomy can fit well within a paradigm that treats privacy as an ongoing, negotiable relationship between the self and the other, or the individual and the community, or between groups of individuals and the wider community. By accepting a relational component to privacy, we can than better understand how to justify claims to privacy that are made in public. This is also largely consistent with Regan’s approach to what she terms the “social value of privacy”, which treats it as having value “not just to individuals as individuals or to all individuals in common”, but also to society itself.\footnote{Regan, supra note 54 at 225.}

As I have noted, boundary conceptions of privacy tend to have a difficult time explaining claims to privacy in public, because they are dependent on people knowing where the \textit{a priori} boundary is – there must be some limit to privacy claims, and so the limitation mechanism is the spatial divide between areas that are public and areas that area private. In contrast, a relational approach to privacy would allow for privacy interests to arise in public as against certain groups but not others – a privacy loss would be understood as a reduction in the ability of an individual to negotiate their distance between themselves and other social actors, and an actionable privacy loss might be one that significantly impinges upon autonomy, as understood from a relational perspective. Thus, the existence of a surveillance system that removes from the individual the power to negotiate their potential exposure to an unseen audience whenever they enter public space would justifiably be understood as a privacy loss. If such surveillance can serve to disrupt or alter a broad range of social relationships in a way that has important implications for personal autonomy, then it might rise to the level of a privacy loss that deserves some kind of legal response.
Much as relational autonomy abandons the idea of a shield to protect personal autonomy, relational privacy also abandons the boundary metaphor. Rather than treating privacy as a protective bubble that is always in danger of being ‘popped’ by an external invasion, it is better understood as a field or blanket that can be strengthened and weakened over time by different practices. The ability to wrap oneself in a ‘privacy blanket’ implies several things. First, that privacy can be shared – the blanket can be drawn around not only yourself, but also those close to you. Second, that privacy can be taken with you – the blanket is something you can choose to wear at all times, wherever you go. Third, that privacy can legitimately be abandoned – the blanket can be discarded, or ‘left at home’. Fourth, that privacy can be weakened and strengthened over time – the blanket can become frayed, but can be repaired. Relational privacy accepts both that privacy has at times a role to play both in creating a personal zone of freedom from unwanted outside interference, and also that it can be used as a means of protecting one’s interactions within a broader community, helping to ensure that the necessary capacities for personal growth and autonomy are properly nourished over time. It also accepts that privacy is something that may be worn down over extended periods of time through repeated low-grade violations, and therefore meaningful privacy rights in a legal sense must seek to guard against such activities, rather than ensuring only protection from direct and obvious ‘invasions’.

This concept still allows for a right to privacy in public that is bounded, rather than being unlimited. An unlimited right to privacy in public, of course, would be implausible – the moment we step outside, we freely share our location, appearance, and behaviours to all those
around us. Nothing in this thesis argues that the everyday existence of participating in public life ought to ground a legal claim against simply being ‘watched’ by those present. Rather, claims to ‘relational privacy’ ought to only be seen as valid where the ability to negotiate exposure to an audience is threatened in a significant way. This allows a distinction to be drawn between a privacy claim against those immediately present, and a privacy claim against those far removed, even though the activity or location over which a privacy right is claimed is identical in both. I suggest that the power to negotiate one’s exposure is not threatened by being ‘watched’ in public space by those immediately present – it is only the unanticipated exposure to an unseen audience of unknown size that does this.450 Thus, the fact that an individual may have been acting ‘in public’, in full view of others – the spatial question – ought not be relevant in determining whether there is a valid claim. Instead, the question ought to be looked at from the relational perspective. In other words, did the reduction in the ability of the individual to adequately negotiate their exposure threaten to harm their autonomy, understood relationally? Did the privacy loss ultimately risk damage to the capacities that allow the individual to act in accordance with “their own choices, values, and identity”?451 This, then, is a dialectical approach to privacy married to relational autonomy.

Can it be said, then, that geo-immersive surveillance impacts upon the ability of an individual to negotiate social interaction in way that harms the kinds of social contexts and relationships that are necessary for the protection or effective exercise of personal autonomy? In other words, can

450 While I believe this is an effective way to think about privacy, as I will argue in the next Chapter, however, when this approach is implemented through tort actions, the result may still be an unwarranted restriction on the expressive behaviour of others. This leads to my conclusion that the better method of legal implementation of a ‘relational privacy’ regime in the context of geo-immersive surveillance is through data protection legislation.  
451 Friedman, supra note 31 at 40.
we understand geo-immersive surveillance as impacting upon relational privacy? I have claimed that geo-immersive surveillance ought to be understood as a privacy loss by virtue of the exposure it creates to an unseen audience, and that this enforced though effectively random exposure limits the capability of people to negotiate their interaction between themselves and society. While they may freely make themselves observable to those in public, they have little to no capability of gauging when that exposure will be dramatically enhanced, thanks to being rendered visible in a geo-immersive image. I have also argued that thanks to this kind of potential exposure to beyond those who are temporally and spatially present, there is the potential for severe consequences in either the form of direct shaming or panoptic impacts on social norm formation. As a result, geo-immersive surveillance can be seen as impacting detrimentally upon the supportive social context spoken of by proponents of relational autonomy. Mackenzie & Stoljar suggest that “oppressive socialization and oppressive social relationships can impede autonomous agency at three interrelated levels”:

1. The processes of formation of an agent’s desires, beliefs, and emotional attitudes.
2. The development of the competencies and capacities necessary for autonomy including capacities for self-reflection, self-direction, and self-knowledge.
3. An agent’s ability to act on autonomous desires or to make autonomous choices.\(^452\)

The potential harms I have identified as being associated with widespread geo-immersive surveillance create the conditions for this kind of oppressive socialization. With regard to the first level, the unintentional internalization of majoritarian norms is a direct interference with the formation of an individual’s beliefs or desires, substituting one social framework in which those beliefs and desires form with another. I argued that potentially the most damaging aspect of this surveillance was its impact on norm formation and transmission, as people (particularly

\(^452\) Stoljar & Mackenzie, *supra* note 422 at 22.
minority groups) begin to internalize sets of norms that appear to be expounded through the surveillance mechanisms, as certain behaviours go unremarked upon while others do not. I further suggested that this internalization could be traced to the panoptic effects associated with geo-surveillance infrastructures, even if that infrastructure does not represent what we typically think of in terms of a Panopticon. Mackenzie & Stoljar note that as regards this first element, a relational approach must take into account “the roles that social norms and institutions, cultural practices, and social relationships play in shaping beliefs and desires.” As I have argued, geo-immersive surveillance indeed threatens to reconfigure social norms in a way that will modify the development and formation of an individual’s desires and beliefs – the process of norm internalization does precisely this.

The oppressive socialization I have argued characterizes increasing deployment of geo-immersive surveillance also has an impact at the second level Mackenzie & Stoljar outline. I noted earlier the multitude of theories that point to the importance of being able to withdraw from the public gaze in order to help self-reflective processes, and if it is accurate to suggest that self development processes cannot be conducted in isolation but rather only through community engagement, to the extent that surveillance retards the ability of individuals to engage in particular ways in public, then those capacities might be retarded. Indeed, I suggested that the effects of surveillance might be felt not only in public spaces, but even behind closed doors, as an individual’s social framework is subtly altered as those around them in the community within which they are embedded alter their behaviour as a result of surveillance. The insidious aspect of norm internalization and Panopticism is that it transfers the effects of surveillance in public

\[453\text{ Ibid.}\]
into permanent aspects of life, whether the cameras are present or not. Finally, the oppressive socialization associated with geo-immersive surveillance directly speaks to the third element – the ability of agents to act upon their autonomous desires. I earlier argued that the fear of online shaming campaigns may impact upon these abilities, even absent overt restriction, as individuals pre-emptively seek to avoid punishment. As Mackenzie & Stoljar specifically argue in reference to this aspect, “autonomy at this level can be impeded not just by overt restrictions on agents’ freedom, but also by social norms, institutions, practices, and relationships.”454 The potential for widespread shaming conducted by anonymous audiences represents a social practice that can restrict autonomy in this sense. The conclusion is, then, that widespread geo-immersive surveillance can be interpreted as a threat to personal autonomy, understood primarily as self-governance, when approached from a ‘relational’ perspective. This is not to suggest that every image taken of an individual is automatically such a threat,455 but rather that the existence of an unpredictable and transient surveillance infrastructure may indeed be.

Summary

Given this potential threat, in the next two chapters I consider two different Canadian legal frameworks that could theoretically apply to geo-immersive surveillance under two different frameworks – tort actions for “invasion of privacy”, and regulation under PIPEDA. I will suggest that in the case of the former, it is clear that the courts have not adopted the many scholarly criticisms of boundary approaches to privacy. Instead, the jurisprudence indicates that

454 Ibid.
455 As I noted in Chapter 2, geo-immersive imagery is used for many positive applications, and it is certainly plausible in certain cases it might actually help bring communities closer, thereby perhaps increasing relational autonomy. For instance, distribution of imagery of poor areas of a city may bring to light chronic underfunding of social services, leading to positive change.
the approach to privacy taken by the courts is one primarily connected to an account of autonomy as independence. It therefore makes heavy reliance upon boundary metaphors, effectively dooming any potential civil action for invasion of privacy as against geo-immersive technology providers. I argue, however, that PIPEDA is not necessarily susceptible to these same criticisms, and may be a more natural vehicle for advancing a ‘relational’ approach to privacy. I suggest that a refocusing of its core principles may be sufficient to allow for adequate regulation of geo-immersive technologies.
Chapter 6: “Invasion of Privacy” Torts & Geo-Immersive Surveillance

In the previous chapters I have considered the development of geo-immersive technologies, and have argued that they represent an emergent surveillance practice that, if left unchecked, could bring with it significant social harms. In the next several chapters, I wish to consider the possibilities for legal regulation as a means of restricting the growth of this surveillance infrastructure. The option I wish to canvass in this chapter is the possibility of private law actions being brought by individuals against the companies that operate the geo-immersive projects, with the idea that this may encourage a shift in corporate behaviour over time if enough actions are successful, or as the result of a court order. The action I intend to study is the tort of invasion of privacy. I intend to demonstrate that in the context of civil actions seeking remedy for a privacy invasion, the essential principle adopted by the courts is that where one has a ‘reasonable expectation of privacy’, one may seek remedy for an unwanted intrusion. Where the intrusion is ‘being watched’, the location of the surveillance (or ‘the watching) is the most important factor in a successful claim. Thus, surveillance in or around an individual’s home, workplaces, or other similar location is typically seen as a violation of their reasonable expectation of privacy (subject to countervailing concerns, such as judicial authorization or workplace security requirements, for instance), while surveillance that occurs in public places generally is not. The Canadian judicial approach to claims for privacy, I conclude, is best understood as one largely dependent on a dichotomy between private and public places.
In this analysis, I will first touch upon the origins of privacy torts in the American jurisprudence, as Canadian judicial authorities often rely upon them when confronted with privacy claims in the civil context. I then go on to outline the statutory torts designed to protect privacy that exist in several Canadian provinces, and consider the likelihood and extent to which such torts might catch the operation of geo-immersive technologies. I will then consider the same claims in the context of the recently adopted common law tort of invasion of privacy in Ontario. In all cases, however, I suggest that the dominance of spatial questions in the reasons of the courts suggest the likelihood of a successful invasion of privacy action being brought against a geo-immersive technology provider is negligible. I therefore conclude the chapter by considering whether an ‘invasion of privacy’ tort could be reinvigorated by the ideas of relational privacy advanced in the last chapter, though my conclusion is that actions in tort are generally ill-suited to remedying the broader social and systemic concerns I have identified.

The Origin of Invasion of Privacy Torts – The American Context

While the focus of this thesis is on the Canadian legal system and the way in which it ought to handle geo-immersive technologies, it is worth considering the American approach as well, as it has had significant influence upon the development of invasion of privacy torts in the Canadian context. Indeed, the origin of the concept of privacy torts is often traced to American legal scholarship, most notably Samuel Warren and Louis Brandeis’ seminal piece “The Right to Privacy”, in which the authors outlined what they saw as a right to privacy that could be found within the common law of the United States. Much as is the case with this thesis, the article

\[456\] Warren & Brandeis, supra note 32.
was written in response to technological developments of the day – the development of equipment that could rapidly develop a photograph, along with an emboldened tabloid press threatened, in Warren and Brandeis’s view, “to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the housetops’.” This possibility, they believed, posed a risk to an individual’s right to be “let alone”, to their “inviolable personality.” They argued that individuals ought to be able to prevent the publishing or dissemination of material about themselves, not because it was their right to profit from it, but because preventing publishing enhanced an individual’s interest in some aspect of their person. Warren and Brandeis found that the American common law already contained the disparate elements of a right to privacy that would protect this interest, but argued that it ought to be explicitly recognized. The ideas contained in “The Right to Privacy” were gradually adopted and expanded by the American courts; writing seventy-five years later, Prosser argued (critically, it should be noted) that even though this was not necessarily the intention of Warren and Brandeis, the American common law had subsequently expanded to reveal four distinct privacy-related torts: intrusion upon the plaintiff’s solitude, seclusion or private affairs; public disclosure of embarrassing facts about the plaintiff; publicity which places the plaintiff in a false light in the public eye; and appropriation of the plaintiff’s name or likeness.

457 Ibid.
458 Ibid.
While there was (and is) debate as to whether these torts were in fact distinctly related to privacy, it is enough to note that this four-part approach has effectively been adopted into the American common law through the Second Restatement of Torts, which reads:

652A. General Principle

(1) One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other.

(2) The right of privacy is invaded by:

   (a) unreasonable intrusion upon the seclusion of another, as stated in 652B; or
   (b) appropriation of the other's name or likeness, as stated in 652C; or
   (c) unreasonable publicity given to the other's private life, as stated in 652D; or
   (d) publicity that unreasonably places the other in a false light before the public, as stated in 652E.

Further guidance is provided within the Restatement as to the ambit of each of these, and as I will show, this approach has had a not insignificant impact upon the development of both statutory and common law privacy torts in other jurisdictions. The unreasonable intrusion upon seclusion standard requires that there is “intentiona[l]” intrusion, “physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns”, but also that “the intrusion would be highly offensive to a reasonable person”. The misappropriation of personality tort requires that the defendant have “appropriate[d] to his own use or benefit the name or likeness of another.” To be liable for publicity given to the private life of another, the defendant must have publicized information that “would be highly offensive to a reasonable person”.

460 Prosser contended, for instance, that while the American common law had evolved this way, none of these four torts were truly related to a distinct understanding of privacy; rather, each protected separate interests such as mental distress (the intrusion tort), reputation (the disclosure and publicity torts), or property (the appropriation tort). In contrast other argued that invasion of privacy ought to be conceived of as a single dignitary tort (see Bloustein, supra note 33 at 188).
461 Restatement (Second) of Torts, § 652A (1977).
person, and [was] not of legitimate concern to the public.”

Finally, the false light variant requires both that the “false light in which the other was placed would be highly offensive to a reasonable person” and that the defendant “had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.”

In the American legal system, “Restatements” of law such as these are not binding in the manner of statutes, but are frequently treated as authoritative sources of law and are regularly cited by the courts; a Restatement is effectively a quasi-codification of the common law. That said, while Restatements are strongly authoritative, this ‘quasi’ element should not be discounted; being the domain of state law, not all American states have accepted all four elements of Prosser’s formulation into their respective common laws, though a number have. As I will show, however, this four-part formulation has resonance outside the American context, and has influenced the development of invasion of privacy torts in other jurisdictions, including Canada.

The Provincial Statutory Torts for Invasion of Privacy

There are four Canadian common-law provinces that have created private law causes of action for invasions of privacy (British Columbia, Manitoba, Saskatchewan, Newfoundland & Labrador), and Quebec has done something similar through its Civil Code and its Charter of Human Rights and Freedoms. The statutes in the common law provinces are generally similar. The Privacy Act in British Columbia, for instance, creates a tort, “actionable without

---

466 Privacy Act, RSBC 1996, c 373. (“The B.C. Act”).
467 The Privacy Act, CCSM c P125 (“The Manitoba Act”).
470 Civil Code of Quebec, SQ 1991, c 64 (“the Q.C.C.”).
471 Quebec Charter of Human Rights and Freedoms, RSQ, chapter C-12 (“The Quebec Charter”).
proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another.\footnote{472} While the B.C. Act does not specifically define what a violation will entail, it does note that it includes “eavesdropping and surveillance, whether or not accomplished by trespass.”\footnote{473} Individuals are deemed to be entitled to a degree of privacy that is “reasonable in the circumstances”, and both the “nature, incidence and occasion of the conduct in question” and the relationship between the parties will assist the court in determining whether a violation of that privacy has occurred.\footnote{474} Statutory defences include consent; that the conduct was in the exercise of a lawful right in defence of property or person or was authorized or required by law; or that the conduct was that of a peace or public officer engaged in their official duties.\footnote{475} There is also a defence for publication of a private matter if the matter was in the public interest or fair comment on a matter within the public interest.\footnote{476} The other common law provincial Acts are much the same, with one notable variation being in the Manitoba Act, which unlike the other statutes requires that there be a “substantial and unreasonable” violation of privacy in order to ground a claim, and also lacks the ‘wilful’ requirement.\footnote{477}

Potential Actions Under the Statutory Torts

It is conceivable that geo-immersive technologies might ground an action in tort under one of the Acts if it could be argued that the public photography associated with them was an ‘unreasonable’ intrusion, given the circumstances, and none of the statutory exemptions applied. However, thus far no case directly on point has been brought in Canada, and so the following

\footnote{472} The B.C. Act, s 1(1).\footnote{473} The B.C. Act, s 1(4).\footnote{474} The B.C. Act, ss 1(2), (3).\footnote{475} The B.C. Act, ss 2(2).\footnote{476} The B.C. Act, ss 2(3)(a).\footnote{477} The Manitoba Act, s 2(1).
analysis will be based on other cases of surveillance, tracking, or similar forms of privacy invasion that relate to the revelation of publicly available information.\textsuperscript{478} While none of these practices share all the characteristics of geo-immersive surveillance, their consideration by the courts under the provincial Acts might offer a predictive guide to a hypothetical case involving commercial surveillance of public spaces.\textsuperscript{479}

My analysis shows, however, that the chance of success for an invasion of privacy claim regarding geo-immersive technologies under one of the provincial statutory torts is low. Recall that under the Acts, \textit{supra}, an individual is presumed to have a ‘reasonable expectation of privacy’, and what is reasonable will vary given the nature, incidence, and occasion of the conduct. The courts place heavy emphasis on the location of the invasion when determining if it violated this reasonable expectation. While on the one hand this makes it easy to resolve ‘obscene’ cases involving so-called ‘peeping toms’ or voyeurs videotaping individuals in bathrooms and bedrooms, it also means that if the detection (or revelation) of personal activities or information is accomplished via observance of public behaviour, there is much greater resistance on the part of the courts to classic it as an invasion of this ‘reasonable expectation.’ This suggests that surveillance of public spaces, even if it reveals details about an individual’s life they would rather keep shrouded, is unlikely to ground a successful liability claim.

\textsuperscript{478} An exception will be cases that relate to employer surveillance of employees. While these cases are interesting, the balancing off of legitimate employer interests in security on their property suggests different calculations than the balancing that occurs in public spaces or private spaces monitored from public vantage points. See for instance \textit{Communications, Energy, and Paperworkers’s Union of Canada, Local 433 v Unisource Canada, Ltd.}, [2004] BCJ No 1261, \textit{Richardson v Davis Wire Industries, Ltd.}, [1997] BCJ No 937, \textit{Doman Forest Products Ltd. v International Woodworkers, Local 1-357}, [1990] BCCAAA No 401, \textit{St. Mary’s Hospital and H.E.U. (Re)}, [1997] BCCAAA No 855, and \textit{Steels Industrial Products v Teamsters, Local 213} [1991] BCCAAA No 500.

\textsuperscript{479} Interestingly, the overwhelming majority of cases come from British Columbia. Whether this is due to it being the jurisdiction with the first Privacy Act is unclear, but it may be the case that British Columbia is something of a test-bed for privacy actions.
However, this focus by the courts on the spatial question does mean that the closer such technologies come to revealing activities within the home, the greater chance there will be of operators of geo-immersive technologies invading an individual’s reasonable expectation of privacy. This analysis goes on to suggest, though, that even if such an invasion were to be found, it seems as though judicial interpretation of the ‘wilfulness’ requirement under the Acts provides a hatch through which geo-immersive service providers could escape liability. My conclusion is, therefore, that the chances of a successful claim under one of the provincial statutory torts for invasion of privacy by an individual subject to geo-immersive surveillance against one of the service providers is negligible.

A Reasonable Expectation of Privacy

Under the provincial statutory torts, the courts place significant importance of an initial spatial or locational question in determining the reasonableness of an individual’s expectation of privacy. However the spatial question is often split – the location of both the subject of the surveillance and the viewer appears relevant. In circumstances where the subject is in an area typically considered ‘private’ and the viewer has invaded that same area in order to conduct the surveillance, then the reasonable expectation of privacy afforded to the subject is considered high. Thus in civil cases involving sexual voyeurism via hidden peepholes or cameras located within a bedroom or hotel room, courts have been quick to find that an individual’s reasonable expectation of privacy has been violated, often awarding significant punitive

\footnote{Such behaviour was not criminalized in the Code until 2005, leaving civil remedies as the primary recourse for victims.}
damages.\textsuperscript{481} In contrast, when the subject is in public spaces, their expectation of privacy is deemed to be much lower. Under the provincial statutory torts, courts have accepted that “there is no reasonable expectation of privacy for actions taking place in public”\textsuperscript{482}; “a person’s reasonable expectation of privacy in his or her own home is ordinarily very high whereas… in a public place [it is] substantially less so”; and that “overt actions and behaviours occurring in public are not really ‘private’ at all.”\textsuperscript{483}

Where the ‘viewer’ is located in public space but the subject of the surveillance is in an area typically treated as more private, however, the calculation is slightly more complicated. In such cases, an individual’s reasonable expectation of privacy may be lowered even though they are on or in private property. For instance, where events on openly viewable private property have been recorded from the vantage point of a public street, one court have found that the individuals recorded have no recourse under the statutory torts for invasion of privacy, arguing that “the salient feature… is the location in which the filming took place. Events transpiring on this parking lot could hardly be considered private in the sense of being shielded form observation by the general public.”\textsuperscript{484} More surprisingly, perhaps, some courts have applied this logic to the interior of private homes that are viewable from the outside, though not consistently.

\textsuperscript{481} See for instance \textit{Lee v Jacobson}, [1992] BCJ No 132 (BCSC) (‘Lee’), reversed however on the ground it could not be established who had made the peephole used to view the sexual activity of the plaintiffs [1994] BCJ No 2459 (BCCA), \textit{Malcolm v Fleming}, [2000] BCJ No 2400 (BCSC) (‘Malcolm’) ($15 000 in compensatory damages and $35 000 in punitive damages awarded to a woman who discovered a video camera placed in her bedroom by her landlord), \textit{LAM v JELI}, [2008] BCJ No 1612 (BCSC) (‘LAM’) (invasion of privacy found after a woman discovered her former partner had made recordings of their sexual activity without consent along with recording images of her daughter changing clothes).

\textsuperscript{482} \textit{Milner v Manufacturer’s Life Insurance Co. (c.o.b. Manulife Financial)}, [2005] BCJ No 2632 (BCSC) (‘Milner’) at para 77.


\textsuperscript{484} \textit{Silber (cob Stacey’s Furniture World) v British Columbia Television Broadcasting System, Ltd.}, [1985] BCJ No 3012 (BCSC) (‘Silber’) at para 17.
For instance, in the context of suspected insurance fraud, a court in B.C. found that even though “a person’s expectation of privacy [is] highest in [their] home”, it was nonetheless lowered in the case at bar because the plaintiff had left “the blinds open and the lights [on]”, meaning anyone could see her.\textsuperscript{485} Other decisions appear to reject this contention, however. In \textit{Wasserman} for instance, the court found that the existence of a property line dispute between neighbours that led to an installation of cameras to ostensibly monitor their mutual fence did not lower the defendant’s reasonable expectation of privacy in his home, the interior of which could be captured by the camera, even though he had initially declined to take any steps to block the camera.\textsuperscript{486} \textit{Wasserman} also suggests that individuals have a reasonable expectation of privacy not only \textit{in} their homes, but also in the immediate vicinity (i.e. on the patio), even though those areas might nonetheless be visible to passers-by. This possibility of reasonable expectations of privacy \textit{outside} the home also appears to have been accepted by the court in \textit{Heckert}, in which the complaint related to a video camera ostensibly installed for security purposes in an apartment building.\textsuperscript{487} The image generated by the relevant camera on the twelfth floor showed the entire common hallway, the elevator doors, and the door to the plaintiff’s unit in the immediate foreground; the images could only reveal the identity of individuals close to the plaintiff’s door, and did not reveal any activities inside the unit.\textsuperscript{488} Walker J. accepted that the plaintiff nonetheless enjoyed a reasonable expectation of privacy in the hallway, even though it was open to anyone who lived in the building and their guests and thus a quasi-public area (or in

\begin{flushright}
\textsuperscript{485} \textit{Milner supra} note 482 at paras 76, 83. Melnick J. also made reference to the lawful authorization of the private investigators as a factor that also lowered the plaintiff’s expectation of privacy, even though that is treated under the B.C. Act as an exemption, rather than a factor in determining the reasonableness of the privacy claim. It is possible that Melnick J. adopted this approach in order to find that the privacy interests of the plaintiff’s daughter \textit{were} violated, even though she too was in her home and had failed to close the blinds.

\textsuperscript{486} \textit{Wasserman v Hall}, [2009] BCJ No 1932 (BCSC) (‘\textit{Wasserman}’).

\textsuperscript{487} \textit{Heckert v 5470 Investments Ltd.}, [2008] BCJ No 1854 (BCSC) (‘\textit{Heckert}’).

\textsuperscript{488} \textit{Ibid} at paras 37-39.
\end{flushright}
the words of the judge, “not truly private”). This is an important shift from the language of the earlier cases, in which any activity in a quasi-public space or viewable to the public necessarily could not attract a privacy interest. While Heckert and Wasserman are interesting developments, it remains generally true however that under the statutory torts, an individual’s reasonable expectation of privacy is only consistently high when they are within a private space that can only be viewed from the outside by surreptitious means. Heckert and Wasserman merely extend this to the immediate vicinity of the home, not public space in general.

Indeed, the general lack of protection for privacy interests in public under the statutory torts is confirmed by cases that do not deal with visual surveillance, but rather claims to privacy over particular information that has been, for whatever reason, brought into the public realm. The courts have concluded that an individual can lose her expectation of privacy over even sensitive information (such as self-taken nude photographs), if she has failed to take necessary steps to adequately protect it or has willingly shared it initially. A reasonable expectation of privacy also cannot be claimed over information that has previously been the subject of legal proceedings. However, some information that has seeped into public space can still be the

---

489 Ibid at para 90.
490 Milton v Savinkoff, [1993] BCJ No 2396 (BCSC), (‘Milton’), in which the plaintiff sought damages under the B.C. Act after the defendant circulated a nude photo of the plaintiff that she had left in a borrowed jacket, implying that the were romantically linked. The court concluded that the plaintiff’s reasonable expectation of privacy over the photograph was eliminated when she failed to initially ask for the photograph to be returned when she discovered the defendant had it, and because she had willingly shared the photograph with an unknown developer in Hawaii in order to get prints (at paras 16-17).
491 In Mohl v University of British Columbia, [2009] BCJ No 1096 (BCCA) (‘Mohl’), leave to appeal to SCC denied, [2009] SCCA No. 340, the plaintiff launched an invasion of privacy claim against the respondent university after it acknowledged to the media that the plaintiff had failed a teaching practicum while registered as a student there. The plaintiff had earlier commenced court actions against the university in an attempt to have the failing mark overturned, leading the Court of Appeal to conclude that “once a person starts a court action, matters which were once private can cease to be so” (at para 16, citing Mohl v University of British Columbia, [2008] BCJ No 1728 (BCSC) at para 11). Since the respondent university was merely confirming information that was already in
subject of a legitimate privacy claim. Where the information is available in public space through no fault of the individual, they may still have a reasonable expectation of privacy over it. In Watts, for instance, the interception of phone calls made from a neighbour’s house was found to be an invasion of privacy. 492 “Notwithstanding that [the telephone calls] were received… over a cordless telephone” and thus the signals emanated into public space with no encryption, allowing for interception of the communications while in public areas, the plaintiff herself had “made the calls in the privacy of her own home and while in her office with the door closed; these calls were not made in a public place where they could easily be overheard.” 493 Thus, even though members of the public could overhear the conversation using a particular device, this was not enough to remove the plaintiff’s reasonable expectation of privacy given its connection to the privacy interests typically associated with the home. While this perhaps is not a striking result, it does at least indicate that at least inadvertently or unwittingly bringing private information into partial public view does not automatically doom an invasion of privacy claim even if certain technology is required to capture it. At the same time, however, it is impossible to deny the importance the court placed on the fact that even though the ‘signals’ existed beyond the confines of the home and were picked up without a physical invasion of the plaintiff’s home, they nonetheless originated from the home.

---

492 Watts v Klaemt, [2007] BCJ No 980 (BCSC) (‘Watts’). The plaintiff’s daughter’s husband had become involved in a dispute with the defendant, leading the defendant to feel threatened enough to start monitoring their phone calls using a scanner and tape recorder. After intercepting a telephone conversation from the plaintiff to her daughter counselling her on how to avoid being detected for welfare fraud, the defendant reported the contents of the conversation to the daughter’s employer, who subsequently terminated her employment.

493 Watts at para 21.
The emphasis by the courts on the low expectation of privacy an individual over (even sensitive) matters they conduct in public or have otherwise brought into quasi-public view (in the case of information) is a consistent feature of the approach by the courts to claims under the statutory torts. The importance of this spatial question under determinations of reasonable expectations of privacy is most likely fatal to any claim related to geo-immersive technologies brought under the provincial Acts. While it is true that Wasserman and Heckert do indicate that the courts are willing to accept that privacy can be invaded in certain situations even when the matter is viewable to the public in some fashion, it still appears to be a very narrow reading connected to the importance of the home and its immediate vicinity. It is true that geo-immersive surveillance can capture images of individuals in the vicinity of their homes, and, though rarely, might also capture images of people within their homes (for instance, through a window or open door). Distinctions can still be drawn, however, between the way in which the ‘vicinity’ cases under the Acts and geo-immersive surveillance operates. In both Wasserman and Heckert, even though the surveillance of the subjects in question was incidental to the operation of the cameras, those cameras still had a relatively narrow field of vision and were continually trained on a fixed area. In contrast, geo-surveillance cameras image broad areas with wide-angle lenses, rather than being focused on a particular individual’s residence. While the courts accepted in Wasserman and Heckert that ‘collateral’ surveillance was still a form of invasion, when such collateral surveillance is combined with the overwhelmingly ‘public’ nature of what geo-immersive technologies attempt to image, it is very difficult to envision an action under one of the provincial privacy statutes gaining much traction. In Wasserman and Heckert, the invasion was conducted using constant video surveillance, rather than rare and random still
photography. Any collateral imaging of the vicinity of residences that characterizes geo-immersive surveillance would likely be considered by the courts to be no more a violation of an individual’s reasonable expectation of privacy under a statutory tort than that of someone taking a photo that happened to have a residence in the background. Likewise, even though the 

information in Watts was drawn from public space, the finding that it was a violation of privacy was closely tied to the fact that the information originated in private circumstances and that the plaintiff had no awareness that her phone calls were being recorded. It is difficult to see how geo-immersive technologies, which overwhelming record public spaces, could be construed by a court to be on the same level of intrusiveness as the surreptitious recording of telephone calls.

The jurisprudence also suggests that in the context of invasion of privacy claims regarding visual surveillance, once the spatial question has been answered by the courts as being ‘public’ or ‘viewable by the public without special measures’, that is effectively the end of a claim to a reasonable expectation of privacy, even though the relevant provincial Acts all define such an expectation to be “reasonable based on the circumstance” (or similar language). Courts appear to treat the spatial question as the only circumstance that can push in the direction of finding liability, so if it does not push in that direction, all other circumstances are irrelevant. All the other factors serve only to push towards a finding of no liability. Milner is a perfect example – despite the location of the invasion in Milner being highly private (the home), other factors (action of plaintiff, relationship between parties) served to remove that expectation of privacy. In contrast, I am unaware of any jurisprudence under the statutory torts in which an individual has been subject to surveillance in an area not considered typically private or within the
Immediate vicinity of that area, but other ‘circumstances’ present have nonetheless meant that
the individual had reasonable expectation of privacy. Whether an expectation of privacy under
the Acts is ‘reasonable under the circumstances’, therefore, is in reality treated by the courts in
the context of surveillance as a question of ‘was this an invasion of an *a priori* private place, and
if so, are there nonetheless reasons we should not find liability?’ The Canadian approach under
the statutory torts therefore relies on ill-defined *a priori* determinations of things or places that
are ‘private’, and therefore offers seemingly no chance of forming the basis of a successful
action against the operators of geo-immersive surveillance.

**Exemptions**

My conclusion is that it is difficult to envision geo-immersive surveillance as successfully
grounding an invasion of privacy tort under any of the provincial Acts. However, if I am wrong
on that question, it is worth considering whether geo-immersive technology service providers
could escape liability through one of the statutory exemptions. Clearly such providers are not
authorized at law, nor are they peace officers undertaking their duties. However, all the Acts
also feature exemptions for invasions that occur in the ‘public interest’. It is certainly
conceivable that operators of geo-immersive technologies may argue that they engaging in
public photography for the benefit of the public – after all, there is no doubt that the services
have proved extremely popular. However, successful reliance on this exemption is usually not
found in situations where the public merely enjoys generalized benefits from the defendant’s
actions; under the jurisprudence, it appears to have been narrowly interpreted so that only the
reporting of events of public interest is a shield against claims for invasion of privacy.494 For

494 *Silber, supra* note 484 at para 23.
instance, when a plaintiff brought suit for invasion of privacy after a video of his hair transplant was broadcast as part of a news segment on treatments for baldness, one of the defendants was able to successfully invoke the public interest exemption under the B.C. Act. At trial, the plaintiff was successful in his claim against the maker of the videotape and the company that sold the videotape to the broadcaster. However, the plaintiff’s claim failed as against the broadcaster on the grounds that not only had they not “wilfully” invaded his privacy given that they had been given assurances (albeit incorrect ones) from the producer of the tape that the plaintiff had consented to its creation, but that the broadcast was also in the “public interest”, one of the statutory exceptions to the Act.

Not being based in reportage or other newsgathering, the typical operation of geo-immersive technologies does not accord with such interpretations of ‘the public interest’, even though many members of ‘the public’ may indeed find the services useful and take great interest in how they develop. It is therefore unlikely that geo-immersive providers that generate imagery for

---

495 Hollinsworth v BCTV, [1996] BCJ No 2638 (BCSC). The plaintiff had consented to the original recording for training purposes, but not to subsequent broadcast.
496 The plaintiff received default judgment due to failure of the maker of the videotape and the company that sold that videotape to the broadcaster to appear, though Drake J. noted that had they appeared he would “have had no hesitation in finding that they violated the plaintiff's privacy”, though no explanation was given as to precisely the nature of invasion he would have found, other than to say that he was entitled to not have his face broadcast. (Hollinsworth at para 24).
497 Hollinsworth, at paras 19-20. On appeal the first of these reasons was affirmed, and so given that the wilful requirement was not met, the Court concluded it was unnecessary to consider whether the broadcast was within the public interest and the exemption ought to apply (though there is little reason to suspect that it was not ([1998] BCJ No 2451 (BCCA) at para 31).
498 Unlikely, though not impossible in isolated instances. For instance, in 2009 a Dutch teenager came across an image while exploring Google Street View that appeared to show him being approached by two individuals from behind; he concluded that the image was of the moments just before he had been mugged, half a year previously. The police requested the original images from Google, who complied, and proceeded to identify and then arrest the individuals depicted. The image was then widely distributed in the news media. See “Google helps net Dutch muggers”, BBC News, Jun 19, 2009, online, http://news.bbc.co.uk/2/hi/europe/8110363.stm, last accessed Jul 7, 2011. If a similar situation were to arise in a Canadian jurisdiction covered by a statutory privacy tort, it is entirely possible that such usage would fall within the ‘public interest’ exemption, regardless of what the image revealed.
their digital maps could rely on the public interest exemption under any otherwise successful statutory tort. However, geo-immersive products that are specifically designed as reportage tools might. For instance NorthStudio360 uses portable geo-immersive equipment to generate detailed records of ‘news-worthy’ events, such as their coverage of the riots in Vancouver that followed the 2011 Stanley Cup Final. The images that make up that coverage clearly show the identifiable, entirely un-blurred, faces of individuals in the crowd. The riot was, however, unquestionably a ‘news event’, and the product provides the public with a unique perspective on how it unfolded, and thus would almost certainly be covered under the relevant statutory exception.

**The New Ontario Common Law Tort for Invasion of Privacy**

The possibility of a successful claim under one of the statutory torts therefore seems unlikely. There is also the possibility, however, that certain jurisdictions might recognize a common law tort of invasion of privacy, one that may not necessarily share the same contours as its statutory counterpart. Indeed, such a tort has now been recognized at the appellate level in Ontario, a jurisdiction that lacks a statutory tort. In this section, then, I canvass the development of this

---


500 There is an initial question, however, as to whether a common law tort of privacy can co-exist with a statutorily created version in a jurisdiction that has adopted one; the jurisprudence on this matter is mixed. In Dawe v Nova Collections Services, a small claims court judge was willing to accept the possibility that at a freestanding tort of invasion of privacy could theoretically exist in the Newfoundland common law independent from the statutorily created version that was present in that jurisdiction ([Dawe v Nova Collection Services (Nfld) Ltd.], [1998] NJ No 22). However, the British Columbia Court of Appeal took a different approach in Mohl, supra. arguing “there is no common-law claim for breach of privacy. The claim must rest on the provisions of the [Privacy] Act.” It is not entirely clear from the reasons whether this means that the existence of the statutory tort in B.C. has entirely foreclosed the possibility of a separate common law tort developing in that jurisdiction, but it is a possibility.

new tort in order to predict its likely scope, and then consider its potential applicability to geo-immersive surveillance.

Privacy interests in Canada, unlike in the U.S., have historically been protected in terms of tort law not through a distinct ‘privacy’ tort, but rather others such as nuisance, trespass, defamation, injurious falsehood, deceit, and passing off.502 There is some similarity between this approach and that of the opponents of Warren & Brandeis, who argued that the American common law was flexible enough to provide privacy-related protections without the need for the recognition of a separate tort. The Canadians courts have historically preferred to subsume privacy claims into an already recognized category of tort, such as private nuisance.503 Some declared, however, that while a free-standing invasion of privacy tort could exist, it was unnecessary to develop such a tort in order to resolve the case before them.504 These early cases illustrate one of the defining challenges courts faced in considering recognition of a freestanding privacy tort – a clear sense of why one was needed; in other words, a set of facts that would have denied a (seemingly justified) remedy to the plaintiff if reliance were placed only on other existing torts. Where the facts could be reconciled with existing torts, it was very difficult to argue in favour of creating a new category of tort. In Krouse, misappropriation of commercial personality seemed

504 See for example Krouse v Chrysler Canada, Ltd., [1972] 2 OR 133-154 (Ont HCJ) (‘Krouse’), rev’d [1973] OJ No 2157 (Ont CA), involving claims regarding the use of a professional football player’s image for commercial purposes without his consent. The plaintiff had argued that in addition to misappropriation of his image, breach of confidence, breach of contract, and unjust enrichment, this was also an invasion of his privacy. At trial Haines J. admitted that while the privacy per se aspect of the case was novel, that alone would not be reason to deny the plaintiff relief and noted that common law had to “grow according to the needs of society” (at para 138). Haines J. went on to conclude that the issue before him could be adequately resolved on the basis of misappropriation of personality and passing off.
a more logical approach, while in *Motherwell*, the invasion of privacy claim fit entirely into the
tort of nuisance. In *Saccone*, a lower court judge seemed more willing to push for creating some
remedy for what he saw as an invasion of privacy, though he did not declare that explicitly that
such an independent tort existed.505

Linden contended (in 2001) that the *Charter* might be a “potential catalyst” for the development
of a common law invasion of privacy tort.506 While this appears to have ultimately been borne out, it has been a long, slow road. Section 8 of the *Charter* provides protections against
unreasonable search and seizure, and in *Hunter* Dickson J. (as he then was) acknowledged that
the purpose of s. 8 went “at least as far” as the protection of privacy for the individual.507
Subsequently, La Forest J. argued in *Dyment* that privacy “is at the heart of liberty in a modern
state” and that it is “grounded a man’s physical and moral autonomy, [and therefore] is essential
for the well-being of the individual.”508 The jurisprudence under the *Charter*, therefore,
“underscores that privacy is a societal value to be protected” and has thereby “provided some
impetus for a limited recognition by some Canadian courts of an independent tort of invasion of
privacy.”509 However, it is certainly not as simple as saying “post-Charter” (or post *Hunter*)
judges instantly felt confident in declaring a common law tort of invasion of privacy to exist; the
dynamic is certainly more complicated. Courts often remained hesitant, perhaps afraid of being

505 See *Saccone v Orr*, [1981] OJ No 3132 (Ont Cty Ct) (*Sacconne*), which involved the recording of a private
telephone conversation and its subsequent playback at council meet that was alleged to have caused the plaintiff
significant embarrassment, Jacob Co. Ct. J. concluded that this was “an invasion of privacy and, despite the very
able argument of defendant’s counsel that no such action exists… the plaintiff must be given some right of recovery
for what the defendant has in this case done” (at para 23).
506 Allen Linden, *Canadian Tort Law* (Toronto: Butterworths, 2001) at p 56.
509 Bell, supra note 502 at 226, 230.
overturned if they were seen as rushing towards the development of a freestanding tort of invasion of privacy without proper justification.\textsuperscript{510}

Nonetheless, by the early 1990s the influence of the \textit{Charter} began to be felt on the development of a common law freestanding tort of invasion of privacy. In the space of two years, Mandel J. penned two different decisions\textsuperscript{511} that advanced a conception of the tort of invasion of privacy. While accepting that there was “no general remedy for infringement of privacy”, he concluded that “whether the invasion of privacy of an individual will be actionable will depend on the circumstances of the particular case and the conflicting rights involved.”\textsuperscript{512}

Mandel J. went on, however, to find that if he was wrong about the invasion of privacy tort, then the cases could both be nonetheless resolved by reference to other, more recognized torts.\textsuperscript{513}

This apparent desire on the part of courts to provide cover for their statements about possible invasions of privacy with reference to the other already recognized torts continued throughout the 1990s.\textsuperscript{514} At the turn of the century then, while it could not be said with certainty that free-

\textsuperscript{510} See for instance \textit{Bingo Enterprises Ltd. v Plaxton}, [1986] MJ No 185, in which Monnim CJM argued that “it would appear that at common law the tort of violation of privacy in regard to disclosure of private information has not been recognized in Canada… This is certainly not a proper or adequate factual situation to develop new law on the tort of invasion of privacy rights at common law” (at p 10). See also \textit{Lord v Canada (Attorney General)}, [2000] BCJ No 1206 (BCSC), in which after being faced with a self-represented litigant, the court concluded that “it is best left to another day, when both sides can provide extensive argument, to definitively conclude whether there is life to this tort” (at para 17).

\textsuperscript{511} \textit{Palad v Pantaleon}, [1989] OJ No 985 (Ont Dist Ct) (’\textit{Palad}’) and \textit{Roth v Roth}, [1991] OJ No 1301 (Ont Ct (Gen Div)) (’\textit{Roth}’).

\textsuperscript{512} \textit{Roth} at para 40. See also virtually identical wording in \textit{Palad}, at p 19.

\textsuperscript{513} In \textit{Palad}, he noted that if he were wrong about the invasion of privacy claim, then the defendant “would [nonetheless] have a cause of action in nuisance and in trespass” (at p 20). In \textit{Roth}, he adopted similar language, suggesting that if he was wrong that a remedy for invasion of privacy ought to lay in such a case, then the same facts could ground a cause of action in harassment or nuisance (at para 44).

\textsuperscript{514} See for instance \textit{Ontario (Attorney General) v Dieleman}, [1994] OJ No 1864 (Ont CJ (Gen Div) (’\textit{Dieleman}’), in which the court concluded (in an interlocutory motion to restrain picketers outside the homes and workplaces of abortion service providers) that while the medical personnel had suffered an invasion of privacy, this was best seen as significant element of nuisance rather than a freestanding tort; \textit{Lipiec v Borsa}, [1996] OJ No 3819 (Ont CJ (Gen Div)), in which the court found that videotaping a neighbour’s backyard in order to record on-going construction
standing invasion of privacy tort existed, it was nonetheless “clear that Canadian courts [did] not hesitate to protect privacy interests under some [other] recognized tort.” In the first decade of the twenty-first century, the results of decisions involving claims based on a freestanding tort of invasion of privacy remained mixed. Some lower courts continued to declare that the law was unclear and sought to resolve the issues before them by reference to another tort, while the Ontario Court of Appeal in Euteneier appeared to conclude that such freestanding tort simply did not exist. Other judicial pronouncements in favour of finding a freestanding tort for invasion of privacy became increasingly bold, however. In Tran, for instance, the court reviewed a number of cases including those cited above and concluded that together they established that an independent tort of invasion of privacy is a “valid” cause of action. In Somwar, Stinson J. concluded that:

Even if the plaintiff's claim for invasion of privacy were classified as “novel” (which, in any event, is not a proper basis for dismissing it) the foregoing analysis leads me to

---

516 See for instance Haskett v Trans Union of Canada Co., [2001] OJ No 4949, in which the court held that “one cannot assert with confidence that there is clear recognition by the Canadian common law of tort of the invasion of privacy as a discrete tort”, and instead characterized the plaintiff’s complaints as an allegation of negligence for breach of duty of care by the defendants (at para s 41, 49); Warman v Grosvenor, [2008] OJ No 4462 (Ont SCJ) (‘Warman’), in which the court concluded the plaintiff had failed to demonstrate how the harm he suffered from an alleged privacy invasion (the publishing online of personal information and a map of his house) was distinct from the tortious conduct that grounded his valid claims of defamation and assault (at para s 67-70).
517 See Euteneier v Lee, [2005] OJ No 3896 (Ont CA) (‘Euteneier’), in which the plaintiff made various complaints after she had been stripped of her clothing by two police officers subsequent to a (lawful) arrest and detention in a video-monitored cell. The defendant police officers were successful at trial and partially successful at the divisional court; however of interest to this discussion is commentary at Court of Appeal, which dealt in part with a cross-appeal from the plaintiff. The cross-appeal was a claim that the trial judge erred by failing to take into account the plaintiff’s privacy and dignity interests when formulating the duty of care standard to be applied. However, the Court of Appeal dismissed this, noting that the evidentiary record and the reasons of the trial judge both indicated this was not the case.
518 Tran v Financial Debt Recovery Ltd., [2000] OJ No 4293 (Ont SCJ) (‘Tran’) at para 38. Tran was reversed by the Divisional Court though not on the invasion of privacy ground, instead finding that Malloy J. had improperly interfered by assisting the unrepresented plaintiff in presenting his case, [2001] OJ No 4103 (Ont SCJ (Div Ct)).
519 Somwar v McDonald’s Restaurants of Canada, Ltd., [2006] OJ No 64 (Ont SCJ) (‘Somwar’).
conclude that the time has come to recognize invasion of privacy as a tort in its own right. It therefore follows that it is neither plain nor obvious that the plaintiff’s action cannot succeed on the basis that he has not pleaded a reasonable cause of action [emphasis mine].

Justice Stinson referred to the four-way American division of the privacy tort, concluding that the plaintiff’s complaint was best classed as an ‘intrusion into [his] private affairs or seclusion’. Somwar, though only a ruling on a motion and therefore of relatively low precedential value, was in 2006 the clearest acceptance then yet made in an Ontario court of a freestanding invasion of privacy tort in the common law, and was subsequently cited with approval in two other decisions at the Ontario Superior Court of Justice.

The slow development in the Ontario courts of a freestanding invasion of privacy tort came to a head in Jones, which stemmed from the improper accessing of the plaintiff’s financial records by the defendant. Sharpe J.A. accepted that the four-part American approach to an invasion of privacy tort was a useful starting point, and suggested that the facts in Jones lent themselves to consideration under the ‘intrusion upon seclusion or into private affairs’ branch. After reviewing the relevant Ontario jurisprudence, considering the impact of the Charter, and reviewing approaches in other common law jurisdictions, Sharpe J.A. concluded that “it [was]
appropriate for [the Court of Appeal] to confirm the existence of a right of action for intrusion upon seclusion.”  

In so doing, he argued that

Privacy has long been recognized as an important underlying and animating value of various traditional causes of action to protect personal and territorial privacy. *Charter* jurisprudence recognizes privacy as a fundamental value in our law and specifically identifies, as worthy of protection, a right to informational privacy that is distinct from personal and territorial privacy.  

Sharpe J.A. went on to outline the elements of this newly recognized tort, adopting the requirements outlined in the American Restatement, *supra*; the “key features” of the action in Ontario are now (1) intentional conduct by the defendant, (2) which results in the invasion of the plaintiff’s private affairs without lawful justification, that (3) a reasonable person would consider the invasion to be highly offensive.  

Sharpe J.A. considered these elements to impose important limitations on the new tort, declaring that a claim for intrusion upon seclusion would only be successful in relatively rare instances, because

Claims from individuals who are sensitive or unusually concerned about their privacy are excluded: it is only intrusions into matters such as one's financial or health records, sexual practices and orientation, employment, diary or private correspondence that, viewed objectively on the reasonable person standard, can be described as highly offensive.  

*Jones* has established, at least in Ontario, that a freestanding tort of invasion of privacy exists, along the lines of the first branch of the American four-part framework – intrusion upon seclusion. In the next section then, I intend to consider whether it is a realistic to imagine that an action against geo-immersive providers could be brought under it, given the parameters outlined by Sharpe J.A.

---

Potential Actions Under the Newly Recognized (Ontario) Common Law Tort

The three requirements outlined in Jones for a successful claim under the newly recognized invasion of privacy tort in Ontario are, again, that the defendant’s conduct was intentional, that the conduct resulted in the invasion of private affairs without lawful justification, and that a reasonable person would find an invasion highly offensive. Given the recent vintage of Jones there is not yet any Canadian jurisprudence that has directly applied it and provided more examples of how these factors might be met. However, Sharpe J.A.’s explicit citation to the American version of the intrusion tort as his model suggests that in addition to looking to interpretations of the provincial statutory torts as a possible predictive model, canvassing some U.S. jurisprudence where relevant may assist in an attempt to envision how an action against geo-immersive technology providers might fair under the new Ontario tort.

Intentional Conduct By the Defendant

There is no doubt that geo-immersive service providers are intentionally conducting their surveillance of public spaces. However, as discussed, they do not intend to actually gather personal information – it is a collateral consequence of a broader operation aimed at digitally recording vast areas of public space. The fact that individuals are recorded in the images is neither necessary to the project nor apparently even desired by the service providers. It is logical that a court applying the new intrusion on seclusion tort might refer to interpretations given to the various provincial statutory torts, given that they too tend to feature something that looks like ‘intent’ requirement; the statutory torts require that the conduct of the defendant have been ‘wilful’, with the exception of Manitoba. Yet, the interpretations given to this wilfulness factor have, as I explained in the previous section, all suggested that the ‘intent’ or ‘wilfulness’
at issue is not the intent to carry out the particular act that may have ultimately led to the plaintiff’s privacy being invaded, but rather a specific intent to actually violate the plaintiff’s privacy. Assuming that a court applying the new common law tort considers interpretations given to the statutory torts relevant in its determination, which I believe is a reasonable assumption, then it is probable that an action against geo-immersive providers under the new tort would fail at the very first step outlined by Sharpe J.A. However, given that it is possible that a court might interpret ‘intent’ as merely intent to undertake the activity that ultimately led to the intrusion, it is worth continuing the analysis through the other steps of the fledgling Ontario tort.

Invasion of Seclusion or Private Affairs Without Judicial Authorization

Under the American version of the tort, invasion of seclusion need not only involve a physical intrusion, though it can. For instance, in the context of a reporter bringing a hidden camera into a psychiatrist’s home-office in order to film him, the court concluded that

[The plaintiff’s] den was a sphere from which he could reasonably expect to exclude eavesdropping newsmen… [While one] takes a risk that [a] visitor may not be what he seems, and that the visitor may repeat all he hears and observes when he leaves [one] does not and should not be required to take the risk that what is heard and seen will be transmitted by photograph or recording, or in our modern world, in full living color and hi-fi to the public at large or to any segment of it that the visitor may select.528

But, the determining factor of whether an intrusion has occurred is not whether a physical place has been violated, but rather “the type of interest involved.”529 This means that the use of equipment may still violate the plaintiff’s privacy rights, even if the defendant is nowhere near the plaintiff at the time the intrusion is alleged to have occurred. For instance, the use of

528 Dietemann v Time, Inc., 449 F 2d 245 (Court of Appeals, 9th Circuit) 1971 (Dietemann), at 249.
parabolic microphones to record the activities of a couple in their bedroom was found to have necessarily “invaded [their] seclusion”\textsuperscript{530}; so does wiretapping a telephone conversation intrude upon seclusion even if the ‘bug’ is not located within the target’s private space.\textsuperscript{531} In general, the American jurisprudence indicates that ‘intrusions’ are not limited only to the ‘physical’ variety, and can also include ‘electronic’ intrusions; “simply put, intrusion is a physical, electronic or mechanical intrusion into someone’s personal life.”\textsuperscript{532} Quite obviously in \textit{Jones} the intrusion was informational, so this is likely to be the approach taken in the Canadian version of the tort as well.

This might be considered a positive thing for a presumptive action against geo-immersive technologies, given that they do not involve a ‘physical’ intrusion into an individual’s private affairs. In reality, however, much like the approach of the Canadian courts with regard to the statutory torts, the American courts have been extremely reluctant to find that any kind of privacy interest has been invaded when the plaintiffs are in public space or otherwise easily viewable by others. In \textit{Gill v Hearst Publishing Co}, for instance, the plaintiffs sued a newspaper after a photograph taken of them in an “affectionate pose” while at an ice-cream stand at the Los Angeles Farmers’ Market was published.\textsuperscript{533} In the court’s view, however, by virtue of being in public the couple had “voluntarily exposed themselves to public gaze in a pose open to the view of any persons who might then be at or near their place of business… [and thus had] waived

\begin{footnotes}
\item[530] \textit{Hamberger v Eastman}, 106 NH 107 (NH Supreme Court) 1964 (\textit{Hamberger}), at 112.
\item[531] \textit{Nader v Gen. Motors Corp.}, 25 NY 2d 560 (NY Court of Appeals) 1970 (\textit{Nader}).
\item[532] Kane, \textit{supra} note 267 at 349.
\item[533] \textit{Gill v Hearst Publishing Co.}, 40 Cal. 2d 224 (Cali SC) 1953 (\textit{Gill}), at 227.
\end{footnotes}
their right of privacy.”

This approach is further confirmed by US jurisprudence related to the third branch of the tort (publicity given to private facts), which though not recognized in Jones may nonetheless influence the development of the intrusion upon seclusion tort in Ontario, given that it requires the existence of ‘private’ facts, much the way the first branch requires evidence of intrusion upon ‘seclusion’ or ‘private affairs.’

As noted under the Restatement’s commentary on the third branch, “there is no liability for giving further publicity to what the plaintiff himself leaves open to the public eye.” The meaning of ‘public eye’ is given a very broad ambit. For instance, a dancer at a strip club who was filmed without her consent and had her image broadcast (though not identified by name) as part of a news segment on a particularly notorious bar in Tennessee alleged that the broadcast invaded her privacy through the public revelation of private facts, as it revealed to her unknowing friends and family that she was an exotic dancer. In dismissing her appeal from a failed claim under the third branch of the invasion of privacy tort, the Sixth Circuit Court of Appeals did not find it necessary to make recourse to the fact that the news segment might have revealed information that was of “legitimate concern to the public” or to any constitutional arguments regarding freedom of the press. Instead, the court simply concluded that since “[the] plaintiff's activities at the club were open to the public, [her] claim for public disclosure of private life was properly dismissed by the district court as a matter of law.” More recently a plaintiff failed in his suit for invasion of privacy after private investigators used a hidden GPS

534 Gill, at 230.
535 Restatement (Second) of Torts, § 652D comment b (1977).
536 Puckett v American Broadcasting Companies Inc., 917 F 2d 1305 (US Court of Appeals, Sixth Circuit) (1990) (‘Puckett’).
537 Puckett, at 6.
device to track his movements by car in the orders of his wife as part of their divorce proceedings. The court concluded that even though the placement of the device was done without the plaintiff’s knowledge, since he never drove the car to a secluded location or one that was out of public view, permanent tracking of his location in no way violated his privacy. As Strahilevitz suggests, then, the general principle in the American jurisprudence is that “public matters [cannot] provide a plaintiff with a cause of action.” It is strains credulity to envision a court concluding that locational information (i.e. a photograph that reveals that Ms. Smith was at the corner of Bay and Front Streets at a particular day and time) about an individual in public is a ‘private’ fact, given that the subjects of such data have clearly made no intention of hiding their presence on public streets. Even behavioural data (i.e. Ms. Smith was revealed doing a particular action) that might be recorded would still have been a behaviour fully advertised to the public present at that moment and space in time. Even if the third branch of the American tort of invasion of privacy were to be adopted by an Ontario court in the future, it would nonetheless appear inapplicable in an action regarding geo-immersive surveillance.

Much like the existing Canadian approach under the statutory torts, then, under the US jurisprudence while a physical intrusion of a private place is not necessary to create a cause of action within the tort, in the context of surveillance or other forms of ‘watching behaviour’, the intrusion must still be into places one is typically believed to have a claim to ‘seclusion’. Again, it is a spatial question dependent on boundary between public and private places. Presuming

538 Villanova v Innovative Investigative Solutions, Inc. No. A-0654-10T2 (Superior Court of New Jersey – Appellate Division), unreported, July. 7, 2011.
539 Ibid, at p 1.
540 Strahilevitz, supra note 202 at 920.
that courts applying the new invasion of privacy in tort in Ontario generally follow their American counterparts (and Sharpe J.A. gave no indication that he believed they should not), this is another reason to believe that any action brought under it against geo-immersive surveillance providers would likely fail. Simply put, they do not ‘invade’ the privacy of an individual in the way that a successful intrusion upon seclusion action requires. At this point, then, a putative action against geo-immersive providers in Ontario under the new tort would seem to have little chance of success, and this is confirmed when consideration is given to the final requirement Sharpe J.A. outlined, that the alleged invasion be considered highly offensive by a reasonable person.

*The Threshold of ‘Highly Offensive’*

The sole American case (currently) involving a lawsuit against Google for invasion of privacy as a result of their geo-immersive programmes turned largely on this issue of the ‘inoffensiveness’ of the imagery generated.541 After discovering photos of their residence on Google Street View despite it being at the end of a private, unpaved road, Aaron and Christine Boring filed suit claiming that Google “significantly disregarded their privacy interests.”542 As the Borings failed to state precisely in their brief which privacy interest (under the four-part framework) it was that was violated, the District Court reviewed the four-part tort framework discussed herein and conclude that only possible options were intrusion upon seclusion and publicity given to private life.543 Regarding intrusion upon seclusion and the requirement of high offensiveness, the court concluded that while many people might resent some of the

542 *Boring* (District Ct) at 699.
543 *Ibid* at 699.
privacy implications of Street View, only “the most exquisitely sensitive... would suffer shame or humiliation.”\footnote{Ibid at 700.} The Borings, the court said, had failed to bring evidence that would demonstrate the reasonable person would be highly offended by publishing images online of their house, and even the Borings themselves had not taken the necessary steps (such as requesting a takedown) with Google to begin eliminating the images.\footnote{Ibid.} The court also suggested that the way in which the Borings had brought suit against Google was evidence that privacy was not their primary concern and that they did not find the images highly offensive or humiliating – truly private people, the court reasoned, would not have begun a lawsuit without obtaining orders to seal the pleadings. By not doing so, information about the Borings (and images of their house) rapidly disseminated through the media once the lawsuit began.\footnote{Ibid.} This failure to successfully plead the ‘offensiveness’ requirement also doomed the claim under the third branch of the tort (publicity given to private facts), and so the court declined to even consider the application of the other elements of that branch (whether or not the facts were private, whether there was publicity given to said facts, whether said facts were nonetheless of public concern).\footnote{Ibid.} On appeal, the Third Circuit Court of Appeals reached the same determination with regard to both branches of the tort, finding that:

\begin{quote}
No person of ordinary sensibilities would be shamed, humiliated, or have suffered mentally as the result of a vehicle entering into his or her un-gated driveway and photographing the view from there... the alleged conduct would not be highly offensive to a person of ordinary sensibilities.\footnote{Boring (Ct. of Appeal), supra note 541 at 3.}
\end{quote}
Sharpe J.A. adopted a relatively similar approach to the question of what a reasonable person would find offensive in Jones, noting that “claims from individuals who are sensitive or unusually concerned about their privacy are excluded.”\textsuperscript{549} It is therefore probable that any action brought in an Ontario court against a geo-immersive provider for the revelation of the typical kinds of imagery generated in geo-surveillance programmes would therefore fail on this ground. Moreover, this is unlikely to change as time progresses – Anderson criticizes the American courts for relying upon empirical determinations of ‘offensiveness’, with the result that privacy is eroded as time goes on; “the more privacy is invaded, the less it is protected.”\textsuperscript{550} The same problem may be true in the Canadian context, given Sharpe J.A.’s adoption of the ‘reasonable person’ standard in determinations of offensive. As photography by Google’s cameras becomes a regular occurrence in almost all major cites, if there is no significant pushback from the citizenry, it will be increasingly difficult to argue that the ‘reasonable person’ does indeed feel the images created are ‘highly offensive.’

Interestingly, while the spatial question is frequently considered under the first step as part of a determination as to whether or not the affairs invaded were in fact ‘private’, in the American jurisprudence it is also sometimes considered under the factor of ‘offensiveness’. Returning to Gill, for example, the court implied there was an important connection between the locational element of the alleged tort (the Farmer’s Market) and whether or not it was an invasion that was, in fact, ‘highly offensive’ to the reasonable person. While the plaintiffs were photographed linked arm-in-arm in a fashion that might be considered an intimate gesture, the California

\textsuperscript{549} Jones appeal, supra note 501 at para 71.

Supreme Court ruled that revealing it in the photograph was not found to meet the ‘highly offensive’ threshold, as it was merely the portrayal of “an incident which may be seen almost daily in ordinary life.” In so doing, the court linked the location of the ‘incident’ and its possible offensiveness; this serves to further privilege the initial spatial question. In Jones, however, Sharpe J.A. did not indicate the spatial location of an alleged intrusion would be relevant under the factor of offensiveness. Instead, he stated that conduct that would meet the ‘highly offensive’ threshold would be that which the reasonable person could see “causing distress, humiliation, or anguish.” Sharpe J.A. went on to provide a (presumably non-exhaustive) list of examples of intrusions that would meet this threshold, including intrusions into “financial or health records, sexual practices and orientation, employment, [or] diary or private correspondence.” However, given that Jones did not involve a spatial invasion but rather an informational one, given the relative closeness to which Jones tacked towards the American tort and the importance given to spatial considerations under the prior Canadian privacy-related jurisprudence, supra, there remains a likelihood that spatial location and the question of offensiveness will be linked in the future.

Immediately, it becomes clear that this is another threshold that appears difficult to meet in the context of any actions under the new tort against the purveyors of geo-immersive surveillance. While it is possible, of course, that images could reveal ‘offensive’ behaviour, in reality, the majority of imagery generated by geo-immersive surveillance is likely to be of the relatively mundane sort. As I have indicated, however, such imagery remains problematic for two

---

551 Gill, supra note 533 at 231
552 Jones appeal, supra note 501 at para 71.
553 Ibid at para 72.
reasons. First, the online disinhibition effect suggests that even relatively ‘mundane’ imagery may lead to uncontrolled sanctioning behaviour. Second, the uneven way in which tertiary image distribution appears to be occurring thus far (often focusing on the ‘everyday’ behaviour of women and minorities, for instance) means that is not only images that show an obvious social transgression that may be subject to viral spread and subsequent mockery. The ‘offensiveness’ requirement of the new tort suggests, then, that it is not a suitable vehicle for remedying concerns related to geo-immersive surveillance.

**The Possible Impact of Aubry**

It is also worth considering the impact of the *Aubry v Editions Vice-Versa*,\(^{554}\) which though a decision from Quebec, may nonetheless have impact on the future interpretation of the Ontario common law invasion of privacy tort. In *Sale v Barr*, for instance, the Alberta Court of Queen’s Bench cited *Aubry* as being “instructive” for recognizing the importance of balancing off “the mutual rights and obligations… protected by the common law and privacy legislation.”\(^{555}\) While not a case of surveillance as traditionally understood, *Aubry* nonetheless grapples with relevant issues of photography in public. Aubry claimed her privacy was invaded after a photograph of her sitting on the steps of a building was published in magazine. Under the Quebec Civil Code, “no one may invade the privacy of a person without the consent of the person unless authorized by law”\(^{556}\), though at the time the photograph was taken, invasion of privacy was only considered a general delict under article 1035 of the old Civil Code.\(^{557}\)

---

\(^{554}\) *Aubry v Editions Vice-Versa*, [1998] 1 SCR 591 (‘Aubry’)

\(^{555}\) *Sale v Barr*, [2003] AJ No 595 (Alta QB) at para 22. This also note-worthy given that the Alberta does not have a statutory privacy tort, suggesting that the potential influence of *Aubry* on the common law is significant.

\(^{556}\) The Quebec Civil Code, Art. 35.

Nonetheless, lacking the more specific direction afforded by the Quebec Civil Code, the Court appears to have relied in some sense on the Quebec Charter to flesh out the understanding of privacy under the prior version, with the majority (L’Heureux-Dube & Bastarache JJ. writing for themselves and Gonthier, Cory, and Iacobucci, JJ.) arguing that “the right to one’s image is an element of the right to privacy” under s. 5 of the Quebec Charter.\(^\text{558}\) Despite this reference to Quebec Charter values, however, both the majority and the dissent accepted that the action still had to meet the requirements of liability under the civil law – fault, damage, and causal connection.\(^\text{559}\)

There was general consensus between the majority and the dissent, on the issue of causation and fault. With regard to the former, the Chief Justice (dissenting) briefly noted that “causality is not at issue here”, while the majority quickly surmised that “no particular problem arises here since the damages are the logical, direct, and immediate consequence of the fault.”\(^\text{560}\) With regard to the issue of fault, the approaches taken by both the majority and the Chief Justice in dissent were broadly similar, and based upon the notion of balancing off competing rights (to privacy and free expression) under the Quebec Charter. The majority first argued that the Quebec Charter’s guarantee of privacy creates a sphere of individual autonomy, and that sphere includes the ability to control the use made of one’s image.

Since the right to one's image is included in the right to respect for one's private life, it is axiomatic that every person possesses a protected right to his or her image. This right arises when the subject is recognizable. There is, thus, an infringement of the person's

\(^{558}\) Aubry, supra note 554 at para 51.

\(^{559}\) Ibid at paras 49, 6, 10.

\(^{560}\) Ibid at paras 27, 66.
right to his or her image, and therefore fault, as soon as the image is published without consent and enables the person to be identified.\textsuperscript{561}

Since the appellants acknowledged they published the photograph without consent and the respondent was easily identifiable in the image, fault existed and the appellants were \textit{a priori} liable. While the majority therefore recognized that the taking of the photograph was an infringement of the right to privacy under the Civil Code, they also argued that it was a right that “[came] into conflict with freedom of expression, which includes artistic expression.”\textsuperscript{562} There were therefore important balancing questions to be answered. L’Heureux-Dube and Bastarache JJ. reasoned that an individual’s “right to respect for private life may be limited by the public’s interest in knowing about certain [personality] traits.”\textsuperscript{563} This is a contextual question – for instance, figures of public renown “can have certain parts of their private life become matters of public interest”, while non-famous individuals also expose themselves to legitimate public interest where they “even if unwittingly, [place themselves] in a photograph in an incidental manner”, such as by attending a public event like a baseball game or a political demonstration.\textsuperscript{564} The balance will also be tipped in favour of the public interest in any situation – significant public event or not – in which the plaintiff was \textit{not} the prime object of the image; the majority found that the public interest “prevails when a person appears in an incidental manner in a photograph of a public place – an image taken in a public place can then be regarded as an anonymous element of the scenery, even if it is technically possible to identify individuals in the photograph.”\textsuperscript{565} In \textit{Aubry}, it was clear that the photographer intended to

\begin{footnotesize}
\begin{enumerate}
\item \textit{Ibid} at para 53.
\item \textit{Ibid} at para 55.
\item \textit{Ibid} at para 57.
\item \textit{Ibid} at para 58.
\item \textit{Ibid} at para 59.
\end{enumerate}
\end{footnotesize}
capture the image of the plaintiff and through his technique he ensured that she was the prime subject of the image – it was not an accidentally or unintentionally created image. This is, of course, the opposite of what happens by processes of geo-immersive surveillance. On a contextual basis, then, the majority found that the invasion of Aubry’s privacy was not justified by any of the balancing factors.

The Chief Justice, though dissenting, also accepted that “the dissemination of [Aubry’s] image constituted a violation of her privacy… [and that] in the abstract this constitute[d] fault.” The question then became, as it did for the majority, to what extent the competing interests of privacy and free expression under the Quebec Charter could be balanced off given the facts of the case. However, under civil liability a mere infringement of a right does not constitute fault; rather, it must be an unjustifiable infringement. The Chief Justice concluded that in Aubry “the public interest [did] not justify the appellant’s fault [since] the appellant could easily have obtained the respondent’s consent”, but failed to do so. She also agreed that “it is possible for the public interest to justify the disseminating of an image of a person who is in a crowd or at the scene of an important event in a purely incidental manner’, but declined to offer specifics of when that would be the case. The Chief Justice’s dissent, therefore, was based on an argument that Aubry had in fact not suffered any obvious damages, with embarrassment before her classmates not reaching the necessary threshold. In contrast, the majority held that even

---

566 Ibid at para 23.
567 Ibid at para 11
568 Ibid at para 27.
569 Ibid.
570 Ibid at para 28.
though the evidence was weak on this point, her embarrassment could still be considered a form of extra-patrimonial damages.\textsuperscript{571}

Ultimately, Aubry received a payment of $2000 for the loss of privacy she had suffered. From the perspective of a claim relating to geo-immersive technologies, the judgment in \textit{Aubry} is mixed. On the one hand it is a positive development from the perspective of privacy advocates in that an individual’s interest in privacy was recognized to exist, at least at some level, when in public. Naturally, the influence of the Court’s statements in \textit{Aubry} about the importance of privacy to the lives of individuals simply when they are going about their daily business and not inviting any extra scrutiny is welcome. At the same time, the Court circumscribed that privacy interest in a fairly narrow fashion, noting that where the image of an individual is incidental, or not the focus of the composition, then that interest will be outweighed by the counter-balancing interests of the public in receiving information and the free expression rights of the artist, \textit{supra}.

The nature of geo-immersive technologies in imaging \textit{everything} within the field of view of the cameras means that individuals caught by them will almost never be the prime focus or subject of any particular ‘composition’. As a result, it is very difficult to envision a successful challenge to their operation under the Quebec Civil Code and the Quebec \textit{Charter}, given the holding in \textit{Aubry}.

McNairn and Scott wrote over a decade ago that while it “remains to be seen what the effect of \textit{Aubry} will be, [the] decision indicates that the Court is prepared to accept that privacy is a value

\textsuperscript{571} \textit{Ibid} at para 71.
essential to the development of private as well as public law principles.” While it may indeed be the case that the Court considers privacy to be a value essential to that development, there is no evidence to suggest that Aubry has had any profound impact on the evolution of invasion of privacy actions outside Quebec in the years since 1998. Despite its seeming recognition of some kind of right to privacy in public, other courts have overwhelmingly relied upon a boundary metaphor of privacy tied closely to spatial questions. Indeed, there is also no obvious route to applying the holding of Aubry to future development of the Ontario common law tort as it was outlined in Jones as a way of modifying it in order that it might be more responsive to geo-immersive surveillance. In the context of tort actions related to geo-immersive technologies, given that the surveillance complained of is overwhelmingly ‘public’ in nature, it is difficult to see such actions meeting the thresholds laid out in Jones, even considering the impact of Aubry. The intrusions upon seclusion are seemingly not ‘intentional’ within the meaning of its past judicial interpretations, they may not actually even be intrusions upon seclusion or private affairs given the import given to the spatial question by courts in both Canada and the US, and they probably do not meet the threshold of highly offensive to the reasonable person, barring rare circumstances that might capture a very particular behaviour. Thus, invasion of privacy torts, in either their current statutory or common law form, is unlikely capture the operation of geo-immersive technologies in Canada.

Canadian privacy law has thus far tended to approach civil claims to visual privacy by asking where an individual was located – if they were in a space seen as appropriately ‘private’, then they are generally granted rights against the intrusion of being placed under surveillance (again, 572 Colin HH McNairn & Alexander K Scott, Privacy Law in Canada (Markham, Ont.: Buttersworths Canada Ltd., 2001) at 49.)
subject to counterbalancing concerns). In contrast, if they are in generally ‘public’ spaces, then they are seen as having little reasonable expectation of privacy in their activities.\(^{573}\) No distinction is made with regard to who is doing the viewing, even if they themselves are spatially and temporally removed from the site of the activity in question – once someone is acting in public, they are deemed to have waived their expectation of privacy. In Chapter 1, I suggested that this type of boundary-metaphor in the context of privacy is reflective of an underlying approach to autonomy that focuses on protecting a person from the collective through a wall of rights, allowing for a zone for freedom of action and personal growth. When this understanding of autonomy underpins a legal tool for protecting privacy vis-à-vis visual surveillance, the relevant authorities appear to envision a ‘barrier’ that is not one that surrounds the person at all times (because such a claim to privacy would be implausible for anyone living in a society where they interact with other people), but rather one that shields activities within presumptively private places. I argued in the previous chapter that a better approach to privacy was a dialectic account that was not dependent on spatial questions in order to determine the legitimacy of the claim. In the next section, then, I consider whether such an approach could be adopted into an invasion of privacy tort. I conclude, however, that it appears very difficult to create a tort that captures the operation of geo-immersive technologies without also capturing a whole host of innocuous behaviour. Moreover, even if such a tort could be devised, it would not be able to respond to the more systemic harms this thesis has identified. I ultimately conclude

\(^{573}\) In the criminal context, however, the court has interpreted sexual voyeurism as applying to surreptitious sexualized photography even if taken in public places, despite the Code’s provision that require the victim be in circumstances that “give rise to a reasonable expectation of privacy”. See Criminal Code, s 162(1), and R v Rocha, [2012] AJ No 163 (Alta Prv Ct).
that private law actions are not the correct vehicle for regulating street photography taken in the context of geo-immersive surveillance.

**A Reconceived Tort**

Even if we are to abandon spatial questions or questions about offensiveness of the subject matter of the image as threshold tests in a reformed invasion of privacy tort, it would still be necessary for tort to successfully capture the operation of geo-immersive surveillance that largely gathers (mostly) innocuous public imagery, without also rendering actionable a whole host of innocuous behaviour – this is the critical tension. On the one hand, as I have already shown, drawing the boundary along presumptively public/private lines would mean an invasion of privacy tort that has no relevance whatsoever for the operation of geo-immersive surveillance, which only in the rarest of cases might reveal an image of an individual *inside* private spaces. At the same time, an invasion of privacy tort based upon a belief that individuals have a reasonable expectation of privacy over *any* activity in public would no doubt successfully capture such operation, but it would also be far too broad. If the action were structured only around *observation*, in theory even watching someone merely with one’s own eyes as they passed by you on the street would be an actionable behaviour (assuming some harm could be proven) under such a tort, a clearly unacceptable result. Assuredly then, there must be some real limits to the situations in which an individual ought to be able to claim a reasonable expectation of privacy while in public. As Austin describes it, “containment anxiety” is a common phenomenon amongst not only privacy theorists but also within the judiciary, as courts resist extension of tort protections for invasions of privacy out of a fear of unduly restricting the
legitimate interests of other parties.\textsuperscript{574} This is a legitimate concern – a hypothetical invasion of privacy tort that allowed for unrestricted claims of privacy in public against an individual who photographed them and made the image available to a far removed audience would have serious consequences for the expressive activities of others.

Lessons from Abroad

Different jurisdictions have therefore adopted different means of limiting the boundaries of invasion of privacy torts or similar actions. In the American context, I earlier discussed how both the threshold test of the invasion being “highly offensive to a reasonable person” and the general elimination of any ‘public affairs’ from the tort is used to limit its scope – in the case of intrusion upon seclusion it is whether the intrusion itself is highly offensive, while in the case of publicity given to private life it is whether the subject-matter disclosed is highly offensive.\textsuperscript{575} Indeed, the elimination of ‘public activities’ from the protection of the torts is not done within a contextual evaluation of whether the individual had a “reasonable expectation of privacy”, but rather as a ‘first principles’ question about when a privacy interest can exist at all.

Certain jurisdictions that have decided to adopt the American framework have also adopted similar techniques for limiting the scope of claims. For instance, the New Zealand Court of Appeal adopted a ‘highly offensive’ threshold test in \textit{Hosking v Runting}.\textsuperscript{576} In \textit{Hosking}, the plaintiffs (a New Zealand ‘celebrity couple’) sought to restrain the publication of photographs of the wife and their 18 month old twins taken without their knowledge while in public; the action

\textsuperscript{574}\textit{Austin, supra} note 37 (‘Privacy & Private Law’) at 3.
\textsuperscript{575}\textit{Restatement of Torts (Second)}, at § 652B and 652D.
\textsuperscript{576}\textit{Hosking & Hosking v Simon Runting & Anor}, [2004] NZCA 34 (NZ Ct of Appeal) (‘\textit{Hosking}’).
was brought against both the photographer and the publisher of a magazine who had commissioned the photographer. The New Zealand Court of Appeal chose to directly adopt the third branch of the American invasion of privacy framework, finding it to be a question of publicity given to private facts (also ruling it was unnecessary for them to decide at that moment “whether a tortious remedy should be available in New Zealand law for unreasonable intrusion into a person’s solitude or seclusion.”)\(^{577}\) The Court limited the scope of the tort by specifying both that the disclosure of the information had to be ‘highly offensive’, and that the information itself was of the type over which an individual had a reasonable expectation of privacy. On this latter ground, the Court of Appeal found that “the photographs taken… [did] not disclose anything more than could have been observed by any member of the public in Newmarket on that particular day” and therefore publication would not reveal “any fact in respect of which there could be a reasonable expectation of privacy.”\(^{578}\) Thus, while adopting the ‘reasonable expectation of privacy’ phrasing that is not common in the US courts, the New Zealand Court of Appeal nonetheless effectively adopted the first principles elimination of public affairs from the ambit of a tort that otherwise matched the third branch of the American framework.

Interestingly, while the American influence on the development in New Zealand of tort actions protecting privacy interests brought with it both the ‘offensiveness’ requirement and the elimination of erstwhile ‘public affairs’ from the scope of the tort, other jurisdictions have not always followed suit. This is particularly the case where the adoption of invasion of privacy torts has been rejected in favour of continued reliance on other actions that might achieve the

\(^{577}\) Ibid at para 118.
\(^{578}\) Ibid at para 164.
same goal. In both Australia and England, for instance, the courts have continued to rely upon the breach of confidence action to deal with issues that might fall under the an invasion of privacy tort in the US. Nonetheless, they have still adopted limiting devices to contain its scope. In *Australian Broadcasting Company v Lenah Game Meats*, the Australian High Court had to consider an application for an interlocutory injunction to restrain the broadcast of a clandestinely made film of an animal processing facility. While the High Court was unable to conclusively explain situations in which activities in public would nonetheless attract a privacy interest, and declined to recognize a tort of invasion of privacy generally, they did indicate an acceptance that public and private are not always mutually exclusive things:

> There is no bright line which can be drawn between what is private and what is not. Use of the term “public” is often a convenient method of contrast, but there is a large area in between what is necessarily public and what is necessarily private. An activity is not private simply because it is not done in public. It does not suffice to make an act private that, because it occurs on private property, it has such measures of protection from the public gaze as the characteristics of the property, the nature of the activity, the locality, and the disposition of the property owner combine to afford. Certain kinds of information about a person, such as information relating to health, personal relationships, or finances, may be easy to identify as private; as may certain kinds of activity, which a reasonable person, applying contemporary standards of morals and behaviour, would understand to be meant to be unobserved.

---

579 *ABC v Lenah Game Meats Pty Ltd*, [2001] HCA 63 (‘Lenah Game Meats’).
580 In a subsequent lower court case, *Grosse v Purvis*, [2003] QDC 151 (District Ct of Queensland) (‘Grosse’). the plaintiff brought an action for, *inter alia*, invasion of privacy after being stalked and harassed by the defendant. Skoien J. reviewed *Lenah Game Meats*, and determined that since the High Court had not foreclosed the development of a freestanding privacy tort, he was free to do so, describing it as a “bold… [but] logical and desirable step” to take (at para 332). In describing the tort, Skoien J. made reference to both the four-part American approach and its consideration by members of the Court in *Lenah Game Meats*, leading him to conclude that to be actionable, an invasion of privacy would have to a willed act that invaded upon the seclusion or solitude of the plaintiff causing detriment or distress, and the invasion would also have to be undertaken “in a manner which would be considered highly offensive to a reasonable person of ordinary sensibilities” (at para 444). However, much like the Canadian jurisprudence, the lower court decisions are mixed. In contrast to the bold proclamation in *Grosse*, see *Giller v Procopets*, [2004] VSC 113 (Sup Ct of Victoria) and *Kalaba v Commonwealth*, [2004] FCAFC 326 (Fed Ct), in which both courts declined to proceed any further than *Lenah Game Meats’* contention that a tort of invasion of privacy may one day emerge.

581 *Lenah Game Meats* at para 42.
The High Court did, however, adopted the ‘highly offensive’ test as a means of limiting the scope of the breach of confidence action, though unlike the American model, the question was whether or not the disclosure rather than the subject matter was offensive. In contrast, a majority of House of Lords in *Campbell v MGN*\(^{582}\) dismissed the idea of using a ‘highly offensive’ threshold, instead arguing that the breach of confidence action ought to apply to information over which the individual had a reasonable expectation of privacy, which in turn was information that was ‘obviously private’. In *Campbell*, a well-known model brought suit for invasion of privacy after a tabloid newspaper published photographs of her leaving a Narcotics Anonymous meeting; ultimately, a majority of the House of Lords found the defendant newspaper group liable for publishing the images. The House of Lords was divided on the result of the appeal, with a central dispute over whether “there was a public interest in [the Mirror’s] publication of information about Ms. Campbell which it would not been justified in publishing about someone else” due to the claimant’s notoriety and repeated statements to the media that she did not use drugs.\(^{583}\) In other words, the question was whether the newspaper owed a duty of confidence with regard to the information (the photographs and details of Campbell’s treatment), and if so, was the claimant’s right to privacy under Article 8 of the ECHR outweighed by the newspaper’s competing right to free expression under Article 10?

Interestingly, while disagreeing on the final result, none of the Lords appeared to adopt a overly strict public/private approach, instead acknowledging that a privacy claim was affected more by the context in which the information was revealed and gathered, and this context was more than

---

\(^{582}\) *Campbell v Mirror Group Newspapers, Ltd.*, [2004] UKHL 22 (‘Campbell’).

\(^{583}\) *Ibid* at para 57.
about location. Lord Nicholls and Lord Hoffman in dissent placed heavy emphasis on the actions of the claimant in engaging with the media with regard to her alleged drug use, thus lowering the reasonableness of her expectation of privacy over the topic (per Lord Nicholls),\textsuperscript{584} or her right to privacy in the relevant areas of her life (per Lord Hoffman).\textsuperscript{585} Lord Hoffman argued, for instance, that a right to privacy would not normally arise in the publication or dissemination of any activities undertaken in public view, though he did accept that one might arise if the dissemination of the activities recorded were particularly humiliating.\textsuperscript{586} The opinions that formed the majority also seemed to reject an outright spatial approach. Lady Hale, for instance, appeared to agree that while public activities typically could not attract a privacy interest, an exception would be made where further dissemination of those activities could cause significant harm to the claimant, which in this case was that the claimant might cease an important drug treatment programme.\textsuperscript{587} Lord Hope acknowledged that ‘general street photography’ was not objectionable on legal basis, but also suggested this was not necessarily true if an identifiable individual was the obvious subject of the photograph; if they were the clear subject, then the question turned to whether disclosure of that image would be ‘offensive’.\textsuperscript{588} Finally, Lord Carswell agreed that the claimant had lowered her expectation of privacy through her dealings with the media, but this did not justify the extent of the disclosure of otherwise confidential information.\textsuperscript{589} While the differing approaches within the Lords’ judgments in \textit{Campbell} makes it difficult to distil any single clear principle, there appeared to be

\begin{footnotesize}
\begin{enumerate}
\item\textsuperscript{584} \textit{Ibid} at paras 31, 24.
\item\textsuperscript{585} \textit{Ibid} at paras 56, 66.
\item\textsuperscript{586} \textit{Ibid} at para 53.
\item\textsuperscript{587} \textit{Ibid} at paras 154-155.
\item\textsuperscript{588} \textit{Ibid} at para 99.
\item\textsuperscript{589} \textit{Ibid} at para 122.
\end{enumerate}
\end{footnotesize}
general consensus that the fact that an activity was viewable by the public or undertaken in a public space was not *automatically* fatal to any claim for privacy over it. On the other hand, their writings indicate that such a claim will only arise in relatively rare situations, most likely where the revelation of the image is particularly offensive or would have dire consequences for the subject. Again, there are limits to the scope of the claim.

The European Court of Human Rights has also held that a privacy right can exist for individuals photographed in public spaces, though it is one that seems closely tied to both the nature of the activity they were undertaking at the moment they were photographed or otherwise visually recorded and the subsequent dissemination of that image. This issue was addressed most directly in *Peck v. United Kingdom*, in which a municipal CCTV camera filmed the applicant during the beginnings of a suicide attempt.\(^{590}\) The municipality later released the CCTV footage to the media, resulting in still photos of the event appearing in newspapers and video footage being broadcast on a programme known as ‘Crime Beat’; the presented narrative was a ‘success’ in which a CCTV operator spotted an individual with a knife and then summoned the police, who were able to intervene and save his life.\(^{591}\) While some blurring was used in the released images and footage in order to protect the applicant’s identity, he was easily recognised by those who knew him personally.\(^{592}\) The applicant requested, *inter alia*, a judicial review of the municipality’s decision to release the footage to the media. This was rejected by the High Court, on the ground that there was no general right to privacy in English law and it was not unreasonable or irrational for the municipality to distribute the footage as a demonstration of the

\(^{590}\) *Peck v United Kingdom*, Application no 44647/98, ECHR (4\(^{th}\) Section), 28/04/2003 (*‘Peck’*).


\(^{592}\) *Ibid* at para 16.
effectiveness of their CCTV programme.\textsuperscript{593} The applicant then contended before the ECHR that the disclosure of the footage by the municipality was in violation of his Article 8 right to privacy.\textsuperscript{594} At the risk of over-simplifying, the core issue before the Court was whether the disclosure of the applicant’s actions in public was an interference with his private life, and if so, whether it was nonetheless in accordance with the law or in pursuit of a statutory objective, and if it was in such accordance, whether the level of interference was justified in a democratic society.

As to whether the recording of the applicant in public was an interference with his private life, the ECHR considered that there is a “zone of interaction of a person with others, even in a public context, which may fall within the scope of ‘private life’” (emphasis mine).\textsuperscript{595} The ECHR also drew an important distinction between the monitoring of individuals in public with and without recording or archiving of the data revealed – the former would not give rise to an interference with an individual’s private life, while the latter might.\textsuperscript{596} Where the individual was a public figure or was attending an event of public interest, then likely even archiving of the images would not constitute such an interference; here, of course, the applicant was in a “public street but he was not there for the purposes of participating in any public event and he was not a public figure.” It is unclear whether this alone would have been enough to constitute interference, because the ECHR placed significant weight on the fact that the complaint in Peck was not about the actual recording or even archiving, but rather the subsequent disclosure. This

\textsuperscript{593} Ibid at paras 29, 32.
\textsuperscript{594} Ibid at para 52.
\textsuperscript{595} Ibid at para 57.
\textsuperscript{596} Ibid at para 59.
was the key factor – while it was true that the applicant was in a public space and did not attempt to hide himself from the cameras or from passers-by, the disclosure of the footage meant “the relevant moment was viewed to an extent which far exceeded any exposure to a passer-by or to security observation that which the applicant could have possibly foreseen” as he walked down the street late at night. 597 Ultimately, the ECHR awarded the applicant 11 800 euros for the non-pecuniary damage associated with the invasion of privacy he suffered, which they deemed to include significant distress, embarrassment, and frustration. 598

*Peck* is interesting in that it offers an account of privacy that is not seemingly dependent on the question of spatial location – the privacy right of the applicant was not eliminated merely by virtue of him being in a public space and viewable by passers-by. Instead, it was accepted that there was distinction between an expectation of privacy vis-à-vis those immediately present and an expectation vis-à-vis those temporally and spatially removed. The English Court of Appeal later expounded on the importance of photography in terms of its connection to privacy in the following manner:

Special considerations attach to photographs in the field of privacy… As a means of invading privacy, a photograph is particularly intrusive. [The] camera, and the telephoto lens, can give access to the viewer of the photograph to scenes where those photographed could reasonably expect that their appearances or actions would not be brought to the notice of the public. 599

The conception of privacy elucidated in *Peck* is one that better accords with the way in which I have suggested geo-immersive surveillance might threaten privacy – the harm is not simply in the moment of the image capture (which is, after all, effectively automated and transient), but

598 *Ibid* at paras 119-120.
599 *Douglas v Hello Ltd (No 3)*, [2006] QB 125 at para 84.
rather in the way in which that fleeting image is archived and rendered accessible to an audience of potentially billions. *Peck* also is more representative of the sort of dialectical approach to privacy I earlier outlined. It suggests that the privacy violation was in part due to removing from the applicant the ability to adequately negotiate the extent of his engagement with the community. While he had accepted that those around him would view him in the city centre, he had not accepted that those activities could be rendered visible to a mass audience, thanks to a combination of CCTV and subsequent broadcast.

But both *Peck* and *Campbell* allow for privacy claims in public only in the most serious of circumstances – the ECHR in *Peck* emphasized the fact that this was public transmission of a suicide attempt, while the majority of the Lords in *Campbell* also placed emphasis on the physical harm that could befall the claimant if she relapsed into drug use if she avoided treatment so as to avoid publicity. In many ways then, this is the threshold of ‘highly offensive’ simply under different phrasing. And yet, as I noted, the kinds of image that typically make up the majority of public street surveillance imagery are almost never going to be of the type that the reasonable person would consider ‘highly offensive’; the overwhelming majority are likely to be innocuous or otherwise non-sensitive. The struggles the courts have with properly limiting the scope identifies one of the great difficulties in developing an effective tort as against public street surveillance, even if one has accepted that privacy has the kind of dialectic aspect I earlier described – you must be able to narrow the scope of the tort so that it accurately identifies those harms that are legally actionable and those that are not without also rendering actionable
innocuous behaviours. In the next section, then, I consider other ways in which the scope of the tort might be drawn so as to avoid this difficulty.

Other Options for Re-drawing the Boundary of the Tort

One option to limit the scope of the tort while still recognizing claims to privacy in public may be to require some kind of intent on the part of the geo-immersive provider to invade the privacy of the claimant. This means of limiting claims is reflected in the existing Canadian privacy jurisprudence, as I have already noted. For instance, the requirement in Aubry that an individual be the prime focus of an image before a privacy claim can attach goes beyond an interest in protecting the expressive rights of others. It has a secondary purpose, one that is also the goal behind the ‘willful’ requirement of the provincial statutory torts. It is a means of directly connecting the harm suffered by the plaintiff to the intentional acts of the defendant. Requiring that the plaintiff be the prime subject of the image is an effective method of ensuring that the defendant did in fact intend to invade their privacy, rather than intended merely to generate a broad image that accidentally recorded an individual. This has the effect of keeping the scope of the privacy interest relatively narrow, but in the context of geo-immersive surveillance, however, also seems to limit the plausibility of any reconceived tort, as the capture of individuals in the images is collateral rather than directly intentional. Much would turn on whether ‘intent’ was interpreted as intent to specifically invade an individual’s privacy or intent only to conduct the activity that ultimately led to that invasion.

Another method of restricting a hypothetical tort might be to consider the kinds of activities that are being undertaken in public, with the notion that one ought to have a reasonable expectation
of privacy over certain activities, but not others. While this is consistent with Peck and Campbell and their emphasis on the ‘private’ nature of the public activity being revealed (suicide attempt and seeking medical treatment, respectively), it is of course contrary to Aubry, which seemed to acknowledge that expectations of privacy in public are not limited to certain kinds of activities. But regardless of prior jurisprudence, this seems problematic for two reasons. First, it suggests that outside of such ‘intensely private’ issues, no reasonable expectation of privacy can be expected. I have suggested, however, that the risks of geo-immersive technologies extend to the revelation of more mundane activities and details of one’s life – I earlier provided examples of how it has subjected women to an intense gaze for the purposes of (apparently) male sexual curiosity or gratification, and how the gaze has been applied to the everyday activities of the poor or ethnic minorities, even in the absence of transgressive behaviour. Second, it fails to acknowledge that individuals do have different expectations of privacy against different audiences, even over the same activities. This thesis is not seeking to suggest that an identical expectation of privacy exists both inside one’s home and outside on the street, but rather that that an individual in public does retain certain privacy interests. The relational approach I outlined earlier seeks primarily to protect the ability of individuals to accurately gauge their exposure – it is the unpredictable exposure to far removed groups that is problematic for this ability, not the decision to enter public space and thus necessarily be exposed to those in the vicinity. In contrast, an approach based on expectations of privacy over specific activities says that certain activities are private regardless of where they take place, and the question of audience is not relevant. In my view, the relevance of the activity being undertaken is not best considered under the initial determination of whether the
individual had an expectation of privacy over it, but rather as a question of the harm suffered – the revelation of certain activities may cause more harm than others, and can properly be considered in the quantum of damages.

What then if we conceive of the reasonable expectation not as being over activities undertaken in public, but rather related to an expectation regarding the method of observation? One might reasonably expect to be watched by anyone else sharing the same public space, but perhaps we might argue that one ought to reasonable expect that your behaviours will not be recorded. This would not capture the innocent ‘people watcher’ in the park – or at least, not one without a camera. But this latter element quickly leads to the conclusion that still without more, the tort would still be overly broad – for instance, without further limitations to its scope, such a hypothetical tort would treat the operation of geo-immersive technologies no differently than an individual tourist taking photographs on a visit to a new city; both are based on the digital ‘recording’ of publicly viewable spaces. Clearly, this would be a draconian and unacceptable limit on the expressive rights of individuals; I do not want to craft a tort that would create a cause of action against a photographer who shares images they have taken of public space, simply because they happen to feature individuals in them. Another possible technique to limit the scope might therefore make reference to the ‘obviousness’ or ‘surreptitiousness’ of the method of observation – for instance, an individual in public might have a reasonable expectation of privacy that she will not be secretly recorded, because such recording removes from them the ability to accurately gauge their exposure and modify their behaviour accordingly. Even though images generated by geo-immersive cameras may not have all of the
implications typically associated with truly clandestine photography (hidden or miniaturized cameras, etc.), one component is similar – a (likely) lack of knowledge that the imaging is going on. But adding this element of ‘surreptitiousness’ still fails to resolve the ‘tourist’ issue – tourists generally do not actively advertise they are taking photographs, and thus many individuals captured in their images may be unaware. At the very least, they are no more obvious in their activities than a ‘Street View’ car with a large camera on its roof is. The fact that it is relatively easy to ‘discover’ that a tourist is taking photographs (i.e. simply by paying attention to them) or that it is possible that one may notice a Street View car on the street does not diminish the reality that such photographs are typically taken without the knowledge of the subjects. So while, the clandestine nature is still an important factor in the kinds of expectations of privacy individuals ought to have in public, it alone is not enough to define its boundaries in useful way.

What then if we suggest that individuals ought to have a reasonable expectation of privacy with regards to the future *distribution* of those images? For instance, an individual might reasonably expect that only those presently in the area can observe and record their behaviours. Future distribution, particularly, digital distribution changes that calculus, by potentially rendering their activities viewable by billions. This gets at much of what makes geo-immersive technologies so risky – the harm is caused not simply by the initial image generation, but rather its subsequent dissemination to an audience far removed both temporally and spatially from the site of the original image. A claim for a reasonable expectation of privacy in public centred around the nature of distribution seems to avoid some of the weaknesses in the other methods I have
described to determine ‘reasonableness’. It can account for the fact that individuals do accept a lower expectation of privacy when in public but without eliminating that expectation entirely – it accepts that individuals lose an expectation of privacy vis-à-vis others in their immediate vicinity, but not vis-à-vis those not present. This also means there is no legitimate complaint about being simply ‘observed’ by others immediately present while in public.

It may be that a combination of the above factors is the most workable approach; indeed, given the ‘contextual’ nature of the reasonable expectation of privacy test, there is no reason to require that we select only one. So, perhaps we can suggest that individuals ought to have a reasonable expectation of privacy in public against being unexpectedly recorded on film or similar medium where the image generated will be broadly shared with the public, and there is no compelling public interest in the distribution. This appears to bring us closer to where we need to be, but unfortunately problems still exist. Distribution of an image to an audience of millions or even billions is no longer the preserve of large corporations – the digital revolution has put the power of that technology in the hands of anyone with a digital camera and access to a computer. As a result, we would still find that such an understanding of reasonable expectation would treat the tourist photographer who subsequently uploaded her images to a photo-sharing website in the same fashion as the commercial operators of geo-immersive technologies. It would do the same for those who took photos of a friend’s birthday party in a park and uploaded them to a Facebook account without securing the consent of every person at the party. It is difficult to argue that distribution in the context of geo-immersive surveillance is not in the ‘public interest’ but that distribution of a privately taken snapshot on Facebook is. Once again, we are
unsuccessful in being able to draw the boundaries of the tort tight enough to include public street surveillance but exclude behaviours for which we do not wish to attach legal liability, even if we accept a dialectical account of privacy that seeks to protect our ability to control our exposure.

The Ineffectiveness of a Private Law Action as a Tool Against Mass Surveillance

I have suggested above that it appears very challenging to design a tort that might capture the operation of geo-immersive surveillance but not more innocuous behaviours, when one adopts an approach to privacy that recognizes claims to privacy in public based on the ability to control our exposure. But in this section, I want to suggest that there are at least two reasons why, even if the boundaries of a hypothetical invasion of privacy tort could be drawn tight enough to include street surveillance but not innocuous public photography, such a tort would still be ineffective as a tool aimed at regulating the kind of mass public surveillance associated with geo-immersive technologies. The first is the systemic rather than targeted nature of the image collection and its connection to the nature of private law actions, and the second is the ineffectiveness of the available remedies as a regulatory tool, if we extrapolate them from existing successful actions for invasion of privacy.

A critical aspect of geo-immersive surveillance is that it is mass surveillance. That is to say, it is not the targeted tracking of a particular individual over a long period of time, but rather the irregular though enforced exposure of random individuals. I have argued, of course, that this can result in harms to both the individuals subject to the surveillance, but also to those living in a society that is increasingly characterized by the existence of a geo-immersive surveillance infrastructure. I suggested that these potential harms mean geo-immersive surveillance can be
understood as threatening the social context within which autonomy can flourish. I also argued that a not insignificant portion of the harm caused by this kind of mass surveillance is due to the possibility of repeated, low-grade privacy violations, rather than obvious or stark privacy invasions. I suggested this means that privacy should be thought of less as a bubble that can be popped, and more of a field that can be strengthened and weakened over time and by different practices. Could the courts therefore develop an approach that looks not just to a single invasion, but rather to a pattern of practices that slowly wear down personal privacy? Could the courts consider ‘systematic surveillance’ under the concept of the ‘nature of the invasion’ in the parlance of the statutory torts? My conclusion is, unfortunately, ‘no’, for both practical and theoretical reasons, and suggests in fact that reliance on private law actions as the best vehicle to regulate the use or deployment of geo-immersive technologies is unwise.

On the practical side, given the irregular nature of how geo-immersive technologies currently operate, it is extremely unlikely that the same commercial provider will photograph the same individual repeatedly. This is further compounded by the fact that the surveillance is undertaken by a variety of commercial providers, meaning one might be captured at one moment by one company, and two months later by another, and one month later by yet another—yet because each individual company photographed the subject only once, it is hard to see how a private law action could be brought against them for the single action, irrespective of whether the overall impact upon the individual in question is properly characterized as repeated or regular surveillance. While it is true that under the statutory torts, the courts have shown willingness to

---

600 Admittedly, this is an unlikely scenario at current levels of deployment. However, it is a useful hypothetical exercise to imagine the way in which private law remedies might respond.
view repeated invasions as an aggravating factor in damage awards, the calculation of harm for the purposes of a damage awards is of course something different than a determination of an individual’s reasonable expectation of privacy. It is difficult to foresee that a court could accept that repeated ‘quasi-invasions’ of privacy (i.e. repeated photography) can add up to an ‘actual’ invasion of privacy (the ‘systematic’ aspect), under a tort based upon a ‘reasonable expectation of privacy’ if none of the ‘quasi-invasions’ were actionable on their own. And if liability could only attach to such independent privacy invasions, then the systematic nature of the surveillance is logically irrelevant to a determination of the expectation of privacy, and would come into play only in determining the quantum of damages. Thus, while I have advocated for an understanding of privacy as a field that can be worn down in certain places over time, it still seems difficult to imagine a tort for invasion of privacy being successfully built around such an idea.

A further difficulty to the nature of private law actions themselves, which are intended to remedy harms suffered by a particular individual or group of individuals. The framing of an action against geo-immersive technology providers under any kind of private law action would require the claimant to explain what harm they have suffered as a result of the actions of the defendant. Simply put, to be successful a private law action must show an identifiable harm suffered by an identifiable plaintiff as a result of the actions of the defendant. It would surely be challenging to successfully argue before a court that an internal, possibly unconscious, decision to modify one’s behaviour was a harm suffered as the direct consequence of an action of a geo-immersive provider. To re-quote Austin, “it is difficult to justify legal coercion to vindicate [a
claim to be insulated from social pressure] interest unless it causes some kind of injury, which explains the popularity of the test that the publicity given to private facts be highly offensive.\footnote{Austin, supra note 37 ('Privacy and Private Law') at 26.}

It is therefore difficult to fit low-grade yet systemic surveillance into a private law framework. As Solove notes, “tort law looks to isolated acts, to particular infringements and wrongs” and is therefore ill suited to remedying such complaints.\footnote{Solove, supra note 174 at 61.} But I have argued that a broad swath of people may be impacted by the deployment of geo-immersive technologies, even if they are not directly recorded in an image. I suggested that the impacts are felt not only by the individuals directly imaged by the cameras, but (as awareness of digital mapping projects increases) may also be felt by those who are not recorded, whose behaviour and norms may nonetheless be shaped by the mere presence of the cameras. They cannot be seen as suffering the required ‘injury’ upon which a successful private law claim must be based. The systemic aspect of the harms for those not caught on camera simply cannot be addressed by private law actions at all, since the necessary connection between the party responsible for the commercial street surveillance and the individual complaining of an impact on their privacy is entirely missing. An individual merely resident in an area subject to repeated photography but who themselves was not photographed would not, surely, have standing before the courts to bring an action against an operator of geo-immersive technologies.

Even in the context of a class action or mass tort proceeding, this would be the case. In a hypothetical class action for invasion of privacy, there would need to be a representative
plaintiff who “would fairly and adequately represent the interests of the class.” In *Markson* the Court of Appeal also established that if potential liability could be established, and it would not be necessary to actually identify which members of the class did in fact suffer the harm. *Markson* related to the charging of criminal levels of interest in the context of money lending, and the Court reasoned that if millions of transactions had be checked manually to discover which class members had in fact been improperly overcharged, the time and cost of determining liability would overwhelm common issues amongst the class. Applied to geo-immersive technologies, then, this principle might indicate that not every individual imaged would have to be identified in order to be a member of the class. However, identifying other members of the class remains challenging. While they would only have to prove they shared common issues, it is hard to imagine that the class would be any more expansive than ‘those imaged by the defendant’, rather than ‘all those who lived in the area where the defendant at one time was operating’, given that the latter would effectively be everyone in every urban area of Canada. In *Pearson v Inco Ltd*, for instance, a trial judge declined to certify an environmental class proceeding on the ground that drawing a line on a map was not a proper way to identify a class that shared common issues. While the decision was ultimately reversed by the Court of Appeal on other grounds, the Court noted with approval the decision by the plaintiffs prior to the appeal to redefine the class as those that had suffered a drop in property values that could be attributed to the environmental harm. This suggests a hypothetical class action against a geo-immersive service provider would still face significant hurdles in properly identifying the class members.

---

603 *Class Proceedings Act*, SO 1992, Chapter 6, s 5(1)(e).
A further complication is that invasion of privacy torts have always been considered a species of intentional torts – those which require a deliberate act on the part of the defendant, in contrast to negligent behaviour. Simply put, none of the harms identified in this thesis are the result of direct or intentional action by geo-immersive providers. It also seems unlikely that the concept of contributory or secondary liability has role to play here – contributory liability in the context of US copyright law holds that a third party may be liable for a harm that they themselves did not cause, if they enabled the harm to occur or benefitted from its occurrence.\textsuperscript{606} If such principles were extended to Canadian tort law beyond the intellectual property context, one might envision Google or another commercial geo-technology provider being held partially liable for the acts of the infringers. However, the American jurisprudence also indicates that contributory infringement will not be found if the product in question that has led to the primary infringement (again, in the case of copyright) is “widely used for legitimate, unobjectionable purposes.”\textsuperscript{607} If this same principle were to be extended into non-copyright claims, then it would appear likely that geo-immersive technology providers could rely upon them to avoid any kind of secondary infringement claim – geo-immersive technology has, after all, wide and varied uses most of which are not harmful.

\textsuperscript{606} See for instance \textit{Gershwin Publishing Corp. v Columbia Artists Management}, 443 F 2d 1159 (2d Circuit 1971), in which the court ruled that “one who, with knowledge of the infringing activity induces, causes, or materially contributes… may be held liable as a contributory infringer” (at para 8).
\textsuperscript{607} \textit{Sony Corp v Universal Studios}, 464 US 417 (1984) at para 45. This case involved allegations that Sony, as a manufacturer of the Betamax video recording system, had helped contribute to the infringement of Universal Studio’s intellectual property via making it easy for home users to duplicate movies. The court found that simply because it was possible that Betamax could be used for copyright infringement could not justify a finding of secondary infringement upon Sony.
A further hurdle to any kind of private law action against geo-immersive surveillance providers relates to the issue of remedies. The remedy for any successful action under an invasion of privacy tort would likely be compensatory damages. As I noted, invasion of privacy torts are intentional torts, and so the issue of remoteness would not be relevant. As a result, if causation of the claimed loss could be established as a result of the intentional acts of a defendant geo-immersive technology operator (though, as I have said, this is highly unlikely), then a damage award is likely to be the remedy. However, the quantum of such an award is likely to be minimal. Under the statutory torts, even the grossest of invasions of privacy (i.e. hidden cameras inside an individual’s bedroom or bathroom) resulted in maximum awards for harm suffered at around $50 000 (Malcolm, for instance, resulted in an award of $15 000 for general damages and $35 000 for punitive damages). The award in Aubry, for an invasion of privacy via photography in public that revealed no intimate or embarrassing behaviour, was only $2000, and that amount was described the by the Court as ‘high’, but not rising to the level of a reversible error – it is safe to assume that future awards for similarly innocuous public photography will be even lower. Reviewing the jurisprudence under the statutory torts up to 2001, McNairn & Scott described the damage awards as ranging from “nominal to moderate”, and there are no cases I have found post 2001 that would change this conclusion.

Of course, the remedy is designed to make the plaintiff whole – that much is not in dispute, and if the courts decide that $2000 is the appropriate amount in light of the alleged privacy violation, then there is nothing unacceptable about that on principle. However, it would not, of course, be a remedy to anyone who had suffered a loss of privacy that was not actionable under this

---

608 McNairn & Scott, *supra* note 572 at 85.
hypothesised tort. And yet, I have argued that these technologies are likely to cause widespread privacy losses thanks to the effects of the surveillant infrastructure, beyond those actually imaged in a photograph. If we rely on actions in tort rather than broader public regulation of these technologies, then to be effective as quasi-regulatory tools they must have a reasonable chance of actually altering broader corporate behaviour. I would suggest however, that they are not likely to. Assuming for the sake of argument that all the difficulties in mounting an action against a geo-immersive provider could be overcome, an award of $2000 against an individual who has invaded the privacy of another through unintentional (in the sense of an identifiable image being collected only in the service of a larger project) street surveillance photography of them in public spaces may indeed be an effective deterrent for future defendants, when they are similarly situated individuals. $2000 is not a crippling financial blow, but it is presumably large enough to make the average photographer think twice before distributing an image they captured of an individual in public without consent that might lead to a privacy claim, if the jurisprudence were to evolve in that direction. But the corporate entities that operate geo-immersive technology programmes on a grand scale are much less likely to be dissuaded from future operation by such small awards. Google, for instance, had a market capitalization of over $180 billion at the time of writing. Its primary competitor in the online mapping space, Microsoft, is similarly massive, with a market capitalization of over $200 billion. While not a perfect measurement of corporate value, the so-called ‘market cap’ levels for the major players in the geo-immersive technology space indicate the simply immense resources they can draw upon in order to initially fight legal battles and if necessary, pay out any damage awards. Given

---

the significant resources that both Google and Microsoft are pouring into geo-immersive technologies, it would be surprising if the threat of paying out the occasional five-figure damage award gave them significant pause. While the major service providers have responded to some privacy concerns (i.e. by agreeing to blur faces and licence plates), there is no evidence that this was in response to the threat of being sued for invasion of privacy.

Of course, it is also possible that repeated successful actions, even if the damages awarded were comparatively minor, might generate enough bad publicity for geo-immersive technology providers that their behavior would be altered; it is difficult to predict with any certainty. Damage awards would also be increased (in an absolute sense) if a successful class action could be mounted; however the success of such an action is not any more likely than a successful standalone case. There is also the possibility of an equitable remedy of injunction being obtained against the company engaged in the surveillance, if a plaintiff could demonstrate that monetary damages were inadequate for some reason, or that irreparable harm would continue. If the injunction were aimed preventing photography from occurring, then it would be difficult for a court to craft such an injunction in a fashion that would both protect a particular individual’s privacy but not have the effect of requiring geo-immersive technology providers to cease operations in vast geographic areas. This problem could be avoided, of course, if an order could be obtained requiring a commercial service provider to remove a particular image. However, commercial providers are already generally willing to remove ‘offensive’ imagery from their service, without a court order. As I noted, the problem is that the imagery tends to quickly circulate beyond the control of the service providers, and it has proven extremely
difficult for individuals to successfully cleanse the Internet of an image, once it has spread. Nonetheless, it cannot be stated unequivocally that the low-level damage awards that I anticipate would be the result of a successful action aimed at geo-immersive technologies under such a tort of invasion doom its effectiveness. Rather, it is merely a factor to bear in mind when attempting to devise legal solutions for real-world problems. However, if the above analysis is incorrect and a tort of invasion of privacy could somehow be crafted that would capture geo-immersive surveillance but not innocuous forms of photography in public, and could also result in awards that changed the behaviour of geo-immersive service providers, then the results might in fact be overly negative. As I have argued, I do not wish to eliminate geo-immersive technologies entirely – they are clearly a valuable service that many Canadians enjoy using for a variety of purposes. I merely wish to limit some of their potential side effects. But developing a successful tort action against geo-immersive technology providers would presumably create a legal action on behalf of every single person captured in geo-immersive imagery. There would be no way for actions in tort to simply limit the frequency with which imagery was collected, since my argument is premised on the idea that everyone retains some form of privacy interest when in public space. If the courts were to recognize this interest, then it might be the end of geo-immersive mapping services in Canada, which is not my desired outcome.

In summary then, it is very difficult to envision a design of a private law action that could adequately ground an action for public street surveillance but not also include innocuous

---

611 Indeed, this can often backfire, in which the efforts to remove the image draw more attention to it. This has been described as the “Streisand Effect”, after the well known singer tried to have an image of her estate removed from a public archive. See “What is the Streisand Effect”, The Economist, online, http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-what-streisand-effect, last accessed May 25, 2013.
behaviour that most people do not believe ought to generate liability. This is the case even if it is based upon the ideas of ‘relational privacy’ I earlier outlined – the nature of photography in public space combined with the possibility of its widespread digital distribution inevitably poses a challenge to our ability to control our exposure to an unseen audience. Moreover, even if such a tort could be designed, the nature of private law remedies mean that not only would it be exceedingly difficult to apply it to the actions of geo-immersive providers, given that the harms stem largely from the actions of the anonymous watchers rather than the image generators, but that it would be totally ineffective as legal tool for anyone suffering from the effects of living in a surveillance society but who is not personally captured by the cameras. On the other hand, if such a tort could be crafted, it might result in the closure of all geo-immersive services, which is not my desired goal. In the next chapter, therefore, I consider whether Canada’s data protection regime, PIPEDA, might be a more useful tool for regulating geo-immersive surveillance.
Chapter 7: PIPEDA, the OPC, & Geo-Immersive Surveillance

In the previous chapters, I have argued that even if we reconceive of privacy in a more ‘relational’ fashion, it is difficult to envision a tort action for invasion of privacy in Canada that can capture the collection and publication of geo-immersive imagery but not also either capture a whole host of innocuous behaviours, or result in the entire shutdown of all geo-immersive mapping efforts. I suggested that this is in part due to a jurisprudential reliance on a conception of privacy that is overly dependent on spatial considerations, connected at least in part to an underlying view of autonomy as ‘independence’. But as I noted in Chapter 1, theories of privacy rooted in the concept of control over personal information are different than those based largely on withdrawal or non-interference, and are not necessarily dependent on those same spatial ideas. I also noted that control regimes are most useful in the commercial context, where they underpin a number of global data protection laws based upon the ‘fair information principles’, including the Personal Information Protection & Electronic Documents Act (PIPEDA). In this Chapter, I note however that surveillance scholars have frequently criticized the fair information principles and data protection law generally as being inadequate to remedy the harms occasioned by surveillance. I will suggest, however, that the bifurcated nature of geo-immersive surveillance in fact makes it plausible that the harms I have identified might in fact be adequately controlled by those fair information principles. Thus, a legal regime based upon a conception of privacy rooted in an individual’s right to control personal information, rather than one that seeks to prevent unwanted intrusions, may therefore be an effective means regulating geo-immersive technologies by commercial entities.
As a result, I go on to consider the application of PIPEDA to geo-immersive technologies. In so doing, I analyze the relevant existing jurisprudence under PIPEDA along with findings made by the Office of the Canadian Privacy Commissioner (‘OPC’) in an attempt to identify the approach the OPC is taking toward the on-going deployment and use of geo-immersive technologies.\textsuperscript{612} I argue that PIPEDA does appear, on its face, to be applicable to the collection of personal information through geo-immersive technologies, and that they likely pass muster under the OPC’s test for ‘reasonableness’. However, I also suggest that the OPC has adopted an essentially minimalist approach to the requirements under Schedule 1 of PIPEDA in the context of public street surveillance. I go on to argue, though, that this flaw is not traceable to the nature of PIPEDA or the fair information principles upon which it is based, but rather to the decision-making of the OPC itself, which may have returned to an emphasis upon an individual’s reasonable expectation of privacy. In conclude that what required is not an entirely new approach, but rather a strengthening of the existing requirements under PIPEDA.

\textbf{Are the Fair Information Principles Relevant in the Context of Surveillance?}

It is first necessary consider two potential objections to reliance on the fair information principles and PIPEDA, rooted in a ‘privacy as control’ approach, as a means to regulate public street surveillance. The first is that privacy as control is a liberal theory still rooted in ideas of

\footnotesize{\textsuperscript{612} The OPC operates on an ombudsman model, responding to complaints on a case-by-case basis. Upon receiving a complaint from a member of the public, the OPC investigates the matter, and determines, \textit{inter alia}, whether the complaint is well founded or not, and whether it has been subsequently resolved. Where the OPC feels that the findings shed light upon the operation of PIPEDA, they are posted on the OPC’s website under the title of either “Findings of the Commissioner” or “Case Summary”. The parties are not named and while the commentary is not binding on any court, it sheds important light on how the OPC sees the rights and duties created by PIPEDA. See for example “Findings under the Personal Information Protection & Electronic Documents Act”, Office of the Privacy Commissioner of Canada, online, http://www.priv.gc.ca/ef-de/pi_index_e.cfm#contenttop, last accessed Oct. 17, 2011.}
withdrawal, unable to account for privacy’s social value. As Lyon has argued, “privacy is very easily construed as an individual matter when in fact it both has profound social aspects and is limited in the extent to which it can deal with the social questions posed by surveillance today.”613 Steeves notes that Westin’s oft-quoted statement regarding privacy being the claim of the individual to control dissemination of information about them, supra, often leaves out the rest of the passage, which reads:

Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small group intimacy or, when among larger groups, in a condition of anonymity or reserve.614 For Westin, then, control over information was a means of enabling this withdrawal. This view of privacy as the power of the individual to withdraw is, of course, the very one I earlier criticized as being overly dependent on metaphors of boundaries and therefore unable to grapple with claims to privacy made in public spaces. Regan, for instance, argues that Westin’s approach (perhaps as emblematic of control theories generally) is still “anchored to the individual… [and suggests that] privacy and social participation are competing desires.”615 In my view, however, ‘control’ is best understood as a means to an end – that is, it was Westin’s chosen method of achieving a state of privacy, understood as the power to withdraw.616 Accepting that the ability to control the circulation of information about oneself in certain contexts may protect privacy does not necessarily require acceptance that privacy is fundamentally a question of the power of the individual to withdraw from society. Indeed, Westin himself acknowledged the social importance of privacy in one sense – he argued that

613 Lyon, supra note 70 at 180.
614 Steeves, supra note at 340 at 195, citing Westin supra note 62 at 7.
615 Regan, supra note 54 at 27.
privacy was just as much a concern of ‘groups’ as it was for individuals. I argue that there is nothing about ‘privacy as control’ or the fair information principles commonly seen to implement that control that is necessarily predicated on a narrow understanding of privacy. Instead, I intend to show that control theories can be used to advance a relational understanding of privacy, even if the mechanism by which that is achieved is through the granting of ‘individual’ rights to control personal information.

The fair information principles were designed primarily to deal with more conventional forms of ‘information privacy’, such as the computerization and processing of financial records. A more powerful critique therefore is that they cannot address the panoptic concerns I considered in Chapter 4 – that is, that harmful social effects can be caused merely by the existence of a surveillance infrastructure, whether or not one’s image is in fact recorded in some fashion. I touched upon these critiques in Chapter 1, noting that a number of surveillance scholars have rejected the idea that ‘privacy’ is a useful antidote to surveillance. It admittedly appears difficult for data protection legislation grounded in the ability to control personal information, such as PIPEDA, to be relevant where no information is actually collected. However, while it may be true that under the fair information principles “it is difficult to contend that a privacy problem per se arises… [when] a structure associated with surveillance does not collect personal information”, I believe the bifurcated infrastructure associated with geo-immersive technologies opens up a possible route to regulation. While that bifurcation is challenging for other reasons, as I have discussed herein, it also increases the possibility that the harms associated with public

\[617\] Westin, supra note 62 at 24.  
\[618\] See Chapter 1, pp. 21-22.
surveillance can be curtailed through timely intervention through data protection legislation based upon the fair information principles. Because the second stage of the infrastructure (the end viewers) is the source of the social harms but is entirely dependent on the imagery generated by the first stage (the commercial service providers), then significantly curtailing the amount and kind of imagery collected can prevent those broad social harms from arising: I have argued herein that the panoptic effects cannot take hold without geo-immersive technologies becoming more widespread and regularized in use.

In this section, then, I want to argue that robust application of the fair information principles to the commercial collection and distribution of the geo-immersive imagery may serve to effectively regulate geo-immersive technologies. This is despite the fact that those principles only apply when personal information is collected, even though I have argued that the social harms associated with visual surveillance extend beyond those actually captured on camera, thanks to panoptic effects. Control-based privacy regimes offer the opportunity to create broadly applicable rules that will have the effect of preventing many of the more serious social harms that would accompany an unrestricted geo-surveillance programme. Even though the fair information principles as implemented under PIPEDA are not applicable in the context of an individual who went unrecorded by a geo-immersive camera, because geo-immersive technologies do collect personal information at least some of the time, they may nonetheless be an effective tool of regulation – if geo-immersive service providers have to meet particular requirements whenever they collect personal information, then that will have the effect of altering the way they operate 100% of the time.

619 I explain my justifications for targeting the service providers rather than end viewers at p. 132 of this thesis.
Thus, while Bennett argues that privacy cannot “halt surveillance” by trying to strike a balance between privacy interests of individuals and organizations, because such an approach is designed to “manage the processing of personal data, rather than to limit it”\textsuperscript{620}, this is not fatal to my purposes here. I am not at all attempting to “halt” the use of geo-immersive technologies – they result in the creation of tools that many people find innovative and useful. I am only seeking that they be properly contained. Likewise, as I have just argued, the bifurcated structure of geo-immersive surveillance means that the proper managing of the amount and frequency of the initial collection of personal information may be possible within the context of the fair information principles. If data protection laws can serve to limit the development of the initial infrastructure, then they may very well serve to prevent the emergence of societal level harms, despite not strictly applying where no information is collected. Flaherty argues that “the effectiveness of data protection [laws] is measured by the extent to which [they] prevent surveillance from having detrimental consequences.”\textsuperscript{621} I suggest that data protection laws, then, may indeed serve as an antidote to certain kinds of surveillance programmes, despite suffering from the apparent weakness of providing only for individual control over personal information.

\textbf{The Applicability of PIPEDA to Geo-Immersive Technologies}

\textsuperscript{620} Bennett, supra note 50 at 494.
\textsuperscript{621} Flaherty, supra note 3 at 11.
PIPEDA is Canada’s primary data protection law in the context of commercial collections of personal information. It is based upon the idea of balancing the privacy interests of Canadians with the legitimate interests organizations may have in their personal information:

The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.622

PIPEDA applies only to (1) “organizations” that (2) in the course of “commercial activities” (3) collect, use, or disclose “personal information”.623 To answer whether geo-immersive technologies meet these initial requirements, I will rely upon Google and Canpages as two paradigmatic examples of geo-immersive technology providers – Google, because it is the largest in the world and most widely used, and Canpages, because it is currently the only Canadian-headquartered operator. The answers should apply, however, to any geo-immersive service provider in the future that operated a service similar to that of Google’s Street View or Canpages’ StreetScene.

Are Geo-immersive Technology Providers ‘Organizations’?

Under PIPEDA and its substantially similar counterparts,624 an “organization” is wide-ranging in scope; it includes an association, partnership, a person, and a trade union, and there are no

---

622 PIPEDA, s. 3.
623 PIPEDA, s 4(1) reads “This Part applies to every organization in respect of personal information that (a) the organization collects, uses, or discloses in the course of commercial activities; or (b) is about an employee of the organization and that the organization collects, uses, or discloses in connection with the operation of a federal work, undertaking, or business.”
624 In short, where the Governor in Council is “satisfied that legislation of a province that is substantially similar” to PIPEDA exists, an organization may be exempted from PIPEDA in regards to the collection, use or, disclosure of personal information within that particular province (PIPEDA, s. 26(2)(b)). Industry Canada has published guidelines outlining the policy and criteria upon which such a judgment will be based; effectively it requires
exemptions granted for small businesses, family-run enterprises, etc.\textsuperscript{625} Under the Interpretation Act, a “person” includes both natural persons and legal persons, such as corporations.\textsuperscript{626} Thus far I have discussed two major players in the geo-immersive technology business in Canada – Google and Canpages. Both are well-known corporations with offices in Canada; clearly they fall within the meaning of “organization” as it is defined by PIPEDA.\textsuperscript{627} This is straightforward, and needs no additional analysis.

**Are the Imaging Operations ‘Commercial Activities’?**

Under PIPEDA, the provisions of the legislation apply to “every organization in respect of personal information that… the organization collects, uses, or discloses in the course of commercial activities”, subject to certain exceptions. Under the language of PIPEDA, “commercial activity” means “any particular transaction, act or conduct or any regular course of conduct that is of a commercial character.”\textsuperscript{628} Any personal information that is not collected, used, or disclosed in the course of commercial activities therefore would escape the requirements of PIPEDA, and the legal analysis would therefore have to shift to alternatives. Google, Canpages, et. al. are all commercial organizations; that much is not in dispute. But

---------------------------
\textsuperscript{625} PIPEDA, s 2(1).
\textsuperscript{626} Interpretation Act, RSC 1985, c I-21, s 35(1).
\textsuperscript{627} The same would undoubtedly hold true for Microsoft, if and when it expands its StreetSide service to Canada (see Chapter 2 for more details on Microsoft’s stated plans).
\textsuperscript{628} PIPEDA, s 2(1).
there is a distinction drawn between being a commercial organization and conducting commercial activities. The Ontario Superior Court of Justice, for instance, has concluded that merely being a business subject to taxation does not determinatively lead to a conclusion that any particular act carried out by that business is “commercial activity” within the meaning of PIPEDA.\(^{629}\) As a result, there may be some question as to whether the imaging and distributing activities, narrowly understood, are in fact “commercial activities” – it is not enough for the purposes of PIPEDA to merely say that Google and Canpages are profit-seeking corporations and thus any activities they undertake are commercial in nature.

It is true that neither company directly charges members of the public for access to the distributed images. Canpages, however, places textual advertisements on its Street Scene webpages; thus, an individual “virtually” exploring Vancouver would see relevant advertisements for local businesses. Given that the Street Scene programme is treated by Canpages as a competitive advantage to drive viewers to its website, and given further that it derives revenue from advertisers on that website, it seems relatively straightforward to declare the distribution of images it collects as being part of “conduct that is of a commercial character.” Canpages only conducts geo-immersive imaging and distribution as a means of furthering its commercial services and therefore PIPEDA is \textit{prima facie} applicable – as the President and CEO of Canpages testified before the Parliamentary Standing Committee on Access to

\(^{629}\) \textit{Rodgers v Calvert} [2004] OJ No 3653 (Ont SCJ) at para 50.
Information, Privacy, and Ethics, “[Canpages] is a business, so there has to be an ultimate commercial purpose.”

The situation with Google, however, is a little more complex. Currently, Street View is (like Canpages) free to the end user, but (unlike Canpages) users are not currently exposed to any advertisements when using the service. In a sense then, there is no obvious commercial operation occurring during either the initial imaging or subsequent dissemination of the images, and so an argument could be made that PIPEDA should not apply. Such a view has at least some support in the jurisprudence. In *State Farm v Canada*, the Federal Court concluded that “the primary characterization of the activity or conduct in issue is… the dominant factor in assessing the commercial character of that activity or conduct.”

One might conceivably argue that the primary characterization of Google’s geo-immersive operations is, at the moment, non-commercial – any personal information that is gathered is not sold or exchanged for anything of value, no individual is required to pay for the service, and there is no third party that currently pays to associate themselves with a particular image in the hopes of generating revenue.

However, it is important to not treat the activities that result in the collection, use, or disclosure of personal information as isolated events, unconnected with the broader mission of geo-immersive technology providers. To reiterate, the definition of commercial activity in PIPEDA includes not only “any particular transaction, act or conduct”, but also “any regular course of

---

631 *State Farm Mutual Automobile Insurance v Canada (Privacy Commissioner)*, [2010] FCJ No 889 (FC) at para 106.
conduct that is of a commercial character.” I argue that Street View is, in fact, part of a regular course of conduct on the part of Google that is of a commercial character, for at least two reasons. First, in its consideration of the applicability of PIPEDA to a social networking service, the OPC accepted that the collection of personal information for the general purpose of enhancing the user experience even without a direct commercial link to the collection of the information itself was still properly characterized as a commercial activity. The collection of personal information by geo-immersive technologies can be interpreted in a similar fashion – it is collected as an adjunct to the overall smooth operation of the service. While OPC Case Findings are not binding on either the Federal Court or future decisions of the OPC itself, they should at least be considered as quasi-authoritative interpretations of PIPEDA.

The second reason for considering geo-immersive technologies as a commercial product (and therefore their information processing as having a commercial character) relates to the concept of ‘halo effect’, drawn from psychological studies that indicate that the perception of one characteristic of another individual can lead a subject to view unrelated characteristics of that individual in either a positive or negative light. This theory has been adapted into the business world, in which a ‘halo product’ is one that draws consumers to a brand, even if as a standalone product it is not necessarily viable or profit making. Effectively, it is a product that creates a particular perception around an organization that helps drive consumer behaviour in a

---


633 See for instance Richard Nesbitt and Timothy Wilson, “The halo effect: evidence for unconscious alteration of judgments” (1977) 35(4) Journal of Personality and Social Psychology 250, in which a university professor who acted ‘friendly’ towards an interviewer was later ranked by undergraduates as having appealing looks, mannerisms, and a pleasant accent. A different group of students was shown the same professor acting in a ‘cold’ manner to the interviewer, and subsequently ranked his looks, mannerisms, and accent as less appealing.
positive manner. Google Street View (again, to simply draw upon it as the paradigmatic example of a geo-immersive technology service) is a perfect example of such a ‘halo product’ – despite generating no revenue whatsoever for Google, the Street View project has become exceedingly well known, helping to cement Google’s reputation as an innovation leader in the digital world. This helps drive traffic to not only the Street View (or ‘Google Maps’) website itself, but to all of Google’s other online properties – including Gmail (Google’s free email service), gCal (their free online calendar), Google+ (their social networking website) and of course Google Search, the most frequently visited website in the world. Google Mail and Google Search provide Google with the bulk of its annual revenue through the use of contextual advertising, and thus Street View can be viewed as another effort to help drive users to those primary websites in two ways. First through the ‘halo effect’, as described – Street View helps cement in the minds of users the idea of Google as an innovative and powerful player in the digital world, encouraging them to turn to Google first. Second, by helping to offer a cohesive portal for Internet users (for instance, the ‘search’ facility within Google Maps and Street View hooks directly into the main Google Search engine, while links to locations can be shared with other users by one click through Gmail and Google+). If one considers Google Street View to be a ‘halo product’ aimed at driving user traffic towards Google’s other revenue generating properties, then it becomes much easier to see it part of a “course of conduct of a

634 See for instance Lance Leuthesser, Chiranjeevs Kohli, Katrin R Harich, "Brand equity: the halo effect measure" (1995) 29(4) Eur J Market 57, describing how the halo effect is a systematic bias in attribute ratings resulting from raters' tendency to rely on global affect rather than carefully discriminating among conceptually distinct and potentially independent brand attributes.
636 See http://www.google.com/calendar.
commercial character.” This approach is also confirmed, in my view, by the decision of the OPC to argue that it is the “core characteristics” of an institution that give rise to either meeting or failing to meet the commercial question. In such instances, even though as an isolated process the collection, processing, and distribution of digital imagery by Google may strictly speaking be non-commercial, its tight connection to the commercial purposes of Google more broadly means that it ought to fall within the ambit of PIPEDA (providing of course that all the other necessary requirements are met).

Even if one discounts this ‘halo effect’ argument, Google’s plans for Street View ultimately include commercial purposes as understood in a more traditional manner. Speaking before the Parliamentary Standing Committee on Access to Information, Privacy, and Ethics in 2009, the managing director and head of Google Canada testified as follows:

> At the end of the day, this product will be part of our mapping portfolio, part of our maps product, and we advertise on maps, or we sell advertising on maps, so we will be absolutely commercializing the product. It's part of a broader strategy to have Google as a platform that can be built upon, and a part of that is giving away a tremendous amount of free service to consumers.

Beyond the obvious possibility for Google to insert advertisements into mapping search results, the groundwork for further commercialization is steadily being laid: in 2010, Google received a U.S. patent that detailed a process by which real estate identified in a Street View image could be ‘claimed’; the owner of the claimed image could then subsequently pay to have a digital advertisement overlaid on part of the image that would be seen by all end users exploring those

---

images online. The patent describes various implementations, all of which are commercial in nature. For example, an owner of a coffee shop could create a link for a digital coupon that could be activated by an end user clicking on the image of the establishment in Street View. Advertisers could display static or animated advertisements over any part of the image, thus ‘updating’ their real world billboards or advertisements; for instance, the patent suggests that the owner of a movie theatre could continually update the “now playing” posters recorded by Street View to show current movies, rather than the out-dated ones captured in the original image, and clicking on those posters would allow the immediate purchase of tickets. The possibilities vast, and demonstrate that Google sees Street View as a core element of its commercial operations, even if currently is not revenue generating.

Whether treated as part of a ‘halo’ aimed at encouraging adoption and use of Google’s other revenue generating properties or as a more conventionally commercial service in the near future, the collection and distribution of digital images of public spaces is best understood as being part of a course of conduct that is essentially commercial character; geo-immersive technologies should therefore be accepted as ‘commercial activities’ within the meaning of the legislation. If the commercial activity and organizational requirements of PIPEDA are met, the next question that must be asked is whether or not geo-immersive providers are in fact collecting, using, or disclosing personal information.

643 Ibid at paras 47, 48.
644 Ibid at para 53.
Do Geo-immersive Technology Providers Collect, Use, or Disclose ‘Personal Information’?

Perhaps the most critical (and possibly the most challenging) threshold that must be met before PIPEDA can be deemed applicable to geo-immersive surveillance is that it must involve the collection, use, or disclosure of ‘personal information’. The OPC has argued that since “the definition of personal information serves as the critical gateway that allows or disallows an individual to invoke his or her right of privacy… a broad interpretation of personal information is justified.” The Federal Court has confirmed this expansive approach in the context of the Privacy Act, which, while applying to the collection, use, or disclosure of personal information by the Canadian government and its various branches rather than the private sector, features effectively the same definition of ‘personal information’ as PIPEDA. IP addresses, voiceprints, photographs, video imagery, employee identification

---

645 PIPEDA, s 4(1).
647 See Canada (Information Commissioner) v Canada (Transport Accident Investigation and Safety Board), [2007] 1 FCR 203 at para 36, citing the approach of La Forest J. (dissenting in the result but followed by the majority on this point, see para 1) in Dagg v Canada (Minister of Finance), [1997] 2 SCR 403 at para 68.
648 The Privacy Act, RSC 1985, c P-21, s 3.
650 See Wansink v Telus Communications, Inc., [2007] FCJ No 122 (FCA) at para 9: “it is common ground that the voice recognition technology used by Telus requires the collection of ‘personal information’ within the meaning of PIPEDA.”
numbers, personal email addresses and content, business email addresses, attendance at a fitness centre, and payload data from Wi-Fi networks, have all been found by the OPC to constitute ‘personal information’. There is no requirement, then, that the information be particularly ‘sensitive’ to be classed as personal. Instead, the crucial question in all cases is whether or not the information in question relates to an identifiable individual; personal information is defined in PIPEDA as being “information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.” This, of course, has the effect of shifting the question to ‘when does information relate to an identifiable individual’? The OPC was successful in arguing before the Federal Court in a case regarding the application of the Privacy Act (again, which features the same definition of ‘personal information’ as PIPEDA) that the test for determining when information was about an ‘identifiable individual’ ought to be “where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information.”

Personal information is not then only that which directly identifies an individual, but is either information about an already identified individual, or information that can lead to the serious

---

656 Randall v Nubody Fitness Centres, 2010 FC 681 (‘Randall’).
658 PIPEDA, s 2(1).
659 Gordon v Canada (Minister of Health), 2008 FC 258 at para 34 (‘Gordon’).
possibility of identification, even if other information is required for successful identification. Thus, the OPC has found that photography of the interior apartment that could be connected to an apartment number was sufficient to count as ‘personal information’ under PIPEDA, even though the images did not include the actual tenants. In making her determination, the Assistant Commissioner noted that

While the purpose of a particular photograph might be to show the state of the walls or the condition of a kitchen or bathroom of a certain unit, it also revealed information about the unit dweller and his or her standard of living. It might show whether they are tidy or not, whether they can afford expensive media equipment or not, whether they love music, or art, or cooking.\footnote{PIPEDA Case Summary #2006-349, supra note 651}

The existing OPC case findings\footnote{Bearing in mind, of course, they that they lack decisive precedential value.} and Federal Court decisions regarding the application of PIPEDA to visual surveillance using cameras of one sort or another suggest that geo-immersive technologies \textit{do} involve the collection of personal information.\footnote{In this section I am considering the findings only as they relate to whether or not the information collected was in fact ‘personal’ for the purposes of PIPEDA. I am not discussing at this stage whether or not the organizations in question were in fact found to have violated the provisions of the Act.} Discrete or covert video surveillance of an individual is inevitably found to trigger the personal information threshold; in a case related to surveillance in connection with an employment dispute regarding the existence of injuries, the OPC found that there was “no question” that this was a collection of personal information\footnote{PIPEDA Case Summary #2004-269, “Employer hires private investigator to conduct video surveillance on employee”, online, https://www.priv.gc.ca/cf-dc/2004/cf-dc_040423_e.asp, last accessed Nov 12, 2012.} and came to a similar conclusion in two other separate findings. The first regarded covert surveillance in order to determine the existence of an improper relationship between two employees,\footnote{PIPEDA Case Summary #2007-388, “Personal relationship between two employees triggers covert surveillance by employer and raises consent issues”, online, https://www.priv.gc.ca/cf-dc/2007/388_20071120_e.asp, last accessed Nov 12, 2012.} while the second also stemmed from an employer hiring a private...
investigator to determine the extent of claimed injuries by an employee receiving benefits. 665

The principle holds true even when the covert collection of information about one individual results in the unintended collection of information about another. 666

But surveillance need not covertly attempt to target a single individual in order to result in the collection of personal information within the meaning of PIPEDA. In one early finding made by the OPC, a company was deemed to have collected personal information within the meaning of PIPEDA when they installed video cameras on the rooftop of its offices and pointed them at a public street. 667 The staff of the organization monitored the video feed and reported to the police any ‘incidents’ they observed, leading the Commissioner to state that “there is no place in our society for unauthorized surveillance of public places by private sector organizations for commercial reasons.” 668 However, the OPC found two years later that the installation by a cable company of a video camera near its offices that broadcast online a live stream of the surrounding street did not result in the collection of personal information. The images were taken with a relatively wide lens and individuals viewing the stream online could neither zoom in or enlarge the image, and thus it was not possible to identify either individuals or licence plates. As a result, the OPC found that the “information captured by the camera did not qualify as personal information for the purposes of the Act.” 669 The factual difference between these

667 PIPEDA Case Summary #2001-1, supra note 652.
668 Ibid.
two cases relates only to the positioning of the camera and whether or not the images revealed could in lead to the identification of individuals. The distinction likely turns then on to the ‘identifiability’ issue – so long as identification is not possible, then the information will not be ‘personal’.

Surveillance that has led to complaints under PIPEDA is not limited to that which occurs in public spaces, of course – the OPC has found that the use of video surveillance cameras to deter shoplifting in a grocery store resulted in the collection of personal information, as did the use of security cameras in restaurants and bars. As already noted, the OPC has also found that still photography of apartments that could be connected to an individual was a record of ‘personal information’. While that case involved only ‘still’ photography of apartments, one PIPEDA complaint arose in the context of video surveillance of a condominium building, ensuring for instance the security of entranceways. The OPC found that “there was no question that the complainant’s personal information, namely, his image, was collected by way of security cameras placed in the condominium and disclosed on the security system monitors.”

A variety of surveillance cases have also cropped up in the employment context, as employers increasingly install video camera based security systems to protect against criminal activity or to monitor employee performance/behaviour. In one, an employee of a railway company

---

672 PIPEDA Case Summary #2006-349, supra note 651.
complained that surveillance cameras installed for ostensibly security purposes were improperly capturing his personal information. In considering the privacy claim under PIPEDA, the Federal Court accepted that even low-resolution images from digital surveillance cameras in a poorly lit area captured personal information; interestingly however, Lemieux J. suggested that the collection of personal information occurred only when the images were viewed, not when they were automatically recorded. In another case, an employee of an Internet service provider complained to the OPC regarding the installation by his employer of web cameras to monitor employees. While the cameras were of low quality, they nonetheless revealed employees in ‘sharp focus’, making it “easy to recognize who they were and what they were doing”; this was found to be a revelation of ‘personal information’. In another case, the complaint related to the installation of several security cameras at a workplace, designed primarily to allow security guards to confirm the identity of employees as they entered the facility. Unlike in Eastmond, the images were regularly monitored ‘live’ by security guards, in addition to being stored digitally for approximately one month, then overwritten unless needed for an investigation. The OPC found this to be a collection of ‘personal information’ within the meaning of PIPEDA (though ultimately concluded that the complaint was not well-founded for other reasons). In a similar case involving the installation of security cameras at a food processing plant, the OPC again concluded that the images generated met the threshold test


675 Eastmond v Canadian Pacific Railway, 2004 FC 852 (‘Eastmond’), at para. 189. I will argue shortly that this was a misguided approach.


of ‘personal information’ and came to the same result in a separate finding regarding the installation surveillance cameras at a bus terminal.

Surveillance cases under PIPEDA are not limited to visual variety, however. For instance, the OPC has also found that information collected from a GPS device is ‘personal information’, because it can be linked to specific individuals (in that case, the drivers of company vehicles equipped with GPS trackers). In that case, the organization in question had added GPS devices to all its vehicles in order to better dispatch and route employees to construction sites. A similar case stemmed from a complaint by a driver employed by a municipal bus system that had also installed GPS devices on its vehicles. While the complaint ultimately failed for other reasons, the OPC found that the threshold test of collecting personal information had was met by the installation and use of these devices to record the locations of individual drivers while on duty. Importantly, these GPS-related cases suggest that the location of an individual can be considered personal information, so long as that location can be linked back to the identity of the individual in question.

Clearly then, various methods of surveillance can lead to the collection, use, or disclosure of ‘personal information’ under PIPEDA. To what extent does the kind of surveillance occasioned by geo-immersive technologies fall within this framework? In other words, which activities

---

undertaken by geo-immersive technology providers might lead to the collection, use, or disclosure of information about an identifiable individual? In Chapter 2, I explained in detail the process by which geo-immersive service providers gather digital imagery – in essence, vehicles with complex camera rigs attached are driven up and down public streets, digital recording multi-directional images at predetermined intervals. The operators of the vehicles have no control over the cameras other than initially turning them on at the beginning of their assigned route and turning them off at the end; the rest of the process is automated, and the drivers of the vehicles have no access to the images recorded while they are driving. The images, however, are digital records not only of the public streets, but also of individuals. If individuals can be identified in the images, then *prima facie* that must be a collection, use, or disclosure of personal information within the meaning of PIPEDA. Such a general principle is confirmed simply by referring to the many OPC Case Findings that hold that visual imagery of an individual is ‘personal information’, *supra*. Figure 22 represents a typical geo-immersive image taken in Toronto.
The only possible factor that would stop the identification of the individuals in the representative image would be the technique of electronic blurring that the service providers have adopted, as outlined in Chapter 2. As I demonstrated, however, the evidence is that the electronic blurring of individual faces is not fool-proof – despite the best efforts of Google’s

---

engineers, they have not reached a 100% rate of automated ‘face identification’, meaning faces often go unblurred. I also noted that even when blurring is successfully applied, it is relatively ineffective in making individuals unidentifiable, particularly to those who know them. It is true that the chances of identifiability of an individual certainly increase in proportion to how well known they are by the viewer of the image.

However, as I explained in my earlier discussion of the idea of the ‘human flesh search engine’, identification of individuals is much simpler when the effort can be, in effect, ‘crowdsourced’. Recall from my examples that one individual with a blurred face was identified thanks to someone recognizing the *wallpaper in his bedroom*, while another photographed only from the knees down was nonetheless identified by a combination of the time and place the photograph was taken along with his shoes. Thus, while I may not personally know the identity of an individual whose face has been successfully blurred by a geo-immersive technology provider, if I share that with a large group, the chances of identification are greatly increased. This is particularly so given that a potential group can be targeted with a relative ease since all the images are tagged with an exact location – if I wanted to successfully identify the individuals in Figure 22, for example, the fact that that they were photographed in the financial district of Toronto during the daytime might suggest possible groups to target who might be able to recognized those individuals despite the blurring. In my view, the information processes associated with geo-immersive surveillance ought to be seen as meeting the standard laid out in

683 By this I mean the ability of the automatic software to understand which parts of a collected image show a ‘face’ and which parts do not. I am not referring to the power of automated software to identify specific individuals in images, which is better termed ‘facial recognition’.
684 See Chapter 3.
Gordon – that they lead to the “serious possibility” of identification for all those recorded in an image, whether they are successfully blurred or not.

To fully answer the question regarding the personal information threshold test, it may also be necessary to distinguish between the collection and disclosure elements. The possibility for the collection of personal information necessarily occurs when the images themselves are taken. But, as I earlier flagged, the finding in Eastmond may be problematic for any argument claiming that geo-immersive technologies are ‘collecting’ personal information; Lemieux J. described the operation of CPR’s surveillance system as follows:

There is no CP official looking at the monitor at the time the cameras are capturing a person's image. Rather, that person's image is recorded on videotape. The recording is never viewed unless there is a triggering event. The recording is wiped out after 96 hours with the result that person's image is never seen if there is no event.\(^{685}\)

Lemieux J. went on to argue that until the images were viewed, no collection of personal information occurred; the use of an automated video surveillance system alone did not trigger PIPEDA.\(^{686}\) A parallel can be drawn from the first stage of CPR’s process to the fashion in which images are collected by geo-immersive technology providers – as noted, it is essentially automatic and the operator has no access to the images after they are recorded. Under Eastmond then, it cannot be said that the process of driving vehicles up and down public streets ‘collects’ personal information within the meaning of PIPEDA. Given that no human ever sees the images until the final distribution (recall that the entire blurring process is also automated, as is the digital ‘stitching’ of the images into an explorable world), we are left with two alternative applications of Eastmond, both of which are unsatisfying and counterintuitive. The first is that

---

\(^{685}\) Eastmond, supra note 165 at para 188.
\(^{686}\) Ibid at para 189.
geo-immersive technology providers do not collect personal information, but only distribute it. The second is that the ‘collection’ occurs at the moment the images are viewed by humans, meaning that the collection of personal information occurs at the exact moment of the distribution, since that is the moment the humans enter the process in a meaningful way.

Both of these seem conceptually unsatisfying. Surely it makes no sense to argue that the gathering of personal information by an organization is beyond the bounds of regulation simply because it is automated and therefore does not properly qualify as ‘collection’. Likewise, it makes no sense to argue that the ‘collection’ occurs several months after the images were actually gathered; if that were the case, why identify collection, use, and distribution in PIPEDA as separate practices? In my view, it was a mistake for the court in *Eastmond* to adopt the concept that viewing by humans triggers the ‘collection’; indeed, it is not even truly consistent with the general principles of PIPEDA, which are clearly aimed at regulating the harvesting of personal information in the context of electronic commerce. Data processing regimes such as PIPEDA grew out of a concern over the use of computerized databanks of information held by organizations, not whether a human was actually involved in the collection of the data in question. As a result, the principles of PIPEDA ought to apply to the collection of images of identifiable images, regardless of whether that collection is automated.

Indeed, subsequent to (and despite) the approach of the Federal Court in *Eastmond*, the OPC appears to have accepted that automated collection of personal information does not escape the boundaries of PIPEDA. Google Street View cars were recently found to have not only been
collecting imagery of the streets upon which they drove, but also ‘payload data’\textsuperscript{687} from open Wi-Fi networks in the area.\textsuperscript{688} The payload information was captured by devices on the vehicles as part of a programme to identify the geographic locations of Wi-Fi hotspots, which could then in turn be used to improve the accuracy of location-based services for individuals using cell phones that lacked a GPS chip or in areas (such as urban zones with multiple skyscrapers) that tended to suffer from poor GPS coverage. The device was intended to merely capture the name and location of the Wi-Fi networks, but a programming error apparently led to the collection of payload information from unsecured (that is, not password protected) Wi-Fi networks, which included “full names, telephone numbers, email addresses, chat sessions, computer passwords, medical listings, etc.”\textsuperscript{689} While not always allowing for perfect identification, the OPC concluded that “the information collected was sufficiently capable of being linked to individuals through data matching or aggregation.”\textsuperscript{690} In its Report, the OPC considered this to be a significant violation of PIPEDA, and the fact that the process was entirely automated was irrelevant. Given that the level of automation used by Google in accidentally capturing this payload data is identical (using the same vehicles performing the same tasks) to that used in the capture of geo-immersive imagery, it is logical to assume that the OPC does not consider it relevant at this point whether or not personal information is ‘collected’ within the meaning of PIPEDA by automated or manual means.

\textsuperscript{687} ‘Payload data’ is content sent over the network; when from an unencrypted network such data can therefore include entire emails, financial details, personal files, etc. – quite simply, any content that is sent over the network. In contrast, headers or metadata, contains only routing instructions on where the information is to be delivered.

\textsuperscript{688} PIPEDA Report of Findings #2011-001, \textit{supra} note 657.

\textsuperscript{689} \textit{Ibid} at para 18.

\textsuperscript{690} \textit{Ibid}.
This also seems to suggest that it is irrelevant for the purposes of PIPEDA whether the
collection of personal information is intentional or accidental (or collateral) in nature. In other
words, Google was not intending to capture the payload data referred to above, and it was a
comparatively small amount of information in terms of raw data when compared to the vast
numbers of high-resolution images it captured at the same time. As a result, it does not seem
likely that a geo-immersive provider could successfully argue that PIPEDA ought to not apply
to its collection of images that show identifiable individuals merely because it was a secondary
(and apparently undesired or unintended) consequence of their primary intention, which is to
record visual space. Given further that it seems relatively uncontroversial to state that geo-
immersive process are also dependent on the distribution of images (as represented by the linked
image of the Toronto intersection, supra) that include identifiable individuals (assuming, of
course, that my argument regarding the inadequacy of blurring is valid), it seems that the
principles of PIPEDA ought to apply to the use, collection, and distribution of imagery
generated by geo-immersive technologies.

**Geo-immersive Technologies & Section 5(3) of PIPEDA: Reasonableness**

I argued above that PIPEDA ought to apply to geo-immersive technologies because they meet
the basic form of an information practice contemplated by the legislation – public street
surveillance is best seen as a commercial activity of an organization that collects, uses, or
discloses personal information within the meaning of the legislation, and there are no apparent
exceptions that are applicable. By virtue of s. 5(1) therefore, geo-immersive technology
providers must comply with the obligations set out in Schedule 1 of PIPEDA. Prior to
consideration of those requirements, I wish to consider whether geo-immersive technologies are
an information practice that would be considered appropriate by a reasonable person, as per s. 5(3). This provision sits outside of Schedule 1, and therefore functions as something of a firewall protecting Canadians from consenting to unreasonable information practices; it states that:

An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.\(^{691}\)

‘Appropriate’ Purposes & the Eastmond Framework

Particularly (though not exclusively) in the context of visual surveillance, the question of reasonableness under s. 5(3) is determined through an application of the ‘Eastmond framework’.\(^{692}\) As explained earlier, Eastmond involved a complaint by an employee of Canadian Pacific Railroads (CPR) regarding the collection of his personal information without consent via video surveillance. CPR contended that the installation of the cameras was for legitimate security purposes, and while the OPC accepted that a stated purpose of ‘security’ was on its face appropriate, they concluded that the application s. 5(3) required a deeper analysis that also looked to the methods in question used to achieve the stated goal. Thus, while the text of s. 5(3) refers only to a question regarding appropriateness of purpose, it has been subsequently interpreted as a requirement for general reasonability of the practice as a whole. The OPC developed a four-part test to determine whether or not, on the whole, an impugned information practice is ‘reasonable’:

1) Is the measure demonstrably necessary to meet a specific need?
2) Is it likely to be effective in meeting that need?
3) Is the loss of privacy proportional to the benefit gained?

---

\(^{691}\) PIPEDA, s 5(3).
\(^{692}\) PIPEDA Case Summary #2003-114, supra note 674.
4) Is there a less privacy-invasive way of achieving the same end?\footnote{Ibid.}

The \textit{Eastmond} framework bears more than a passing resemblance to the \textit{Oakes}\footnote{\textit{R v Oakes}, [1986] 1 SCR 103 (‘\textit{Oakes}’).} test, which was developed by the Supreme Court of Canada as a method of determining when an infringement of a Charter right would be acceptable under s. 1.\footnote{Section 1 states “The \textit{Canadian Charter of Rights and Freedoms} guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.” The \textit{Oakes} jurisprudence evolved in order to explain what these limits would be.} \textit{Oakes} requires a two-stage analysis. In the first stage, the court asks whether or not the objective was pressing and substantial in a free and democratic society. The second stage is known cumulatively as the ‘proportionality test’, and requires proof of the following:

First, the measures adopted must be carefully designed to achieve the objective in question. They must not be arbitrary, unfair or based on irrational considerations. In short, they must be rationally connected to the objective. Second, the means, even if rationally connected to the objective in this first sense, should impair “as little as possible” the right or freedom in question. Third, there must be a proportionality between the effects of the measures which are responsible for limiting the Charter right or freedom, and the objective which has been identified as of “sufficient importance”.\footnote{\textit{Oakes}, supra note 694 at para 70.}

The \textit{Eastmond} framework tacks relatively closely to this – the ‘pressing and substantial objective’ maps on to the ‘demonstrably necessary’ requirement, while the proportionality analysis in \textit{Oakes} essentially maps on to the third and fourth steps of \textit{Eastmond}. On this basis, a determination as to whether the purposes of the relevant information practice are in fact appropriate is made by reference to not only a basic definition of the purpose or need behind the information practice in question, but also to the methods used to achieve it and, under the rubric of proportionality, a consideration of whether a successful balance is struck between the needs of the organization and the privacy interests of the individual. In its original investigation into
CPR’s use of security cameras in its rail yards, the OPC concluded that since there were only minor incidents of vandalism, CPR had failed to demonstrate the existence of a genuine security threat that necessitated the installation of the cameras, and that there was a lack of evidence that the cameras were in fact effective in reducing vandalism. The question of the reasonableness of the practice therefore failed on the first two steps of the framework. When CPR declined to remove the cameras, the employee went to the Federal Court (as was his right under PIPEDA) to seek enforcement of the OPC’s finding and removal of the cameras.

The Federal Court adopted the same four-part test, accepting that the “appropriateness of purposes… must be analysed in a contextual manner, looking at the particular circumstances of why, how, when and where collection takes place.” In applying it, however, the Federal Court came to the opposite conclusion than had the OPC, determining that “a reasonable person would consider [CPR’s] purposes for collecting [the images]… appropriate in the circumstances.” First, the Federal Court accepted that the evidence before it indicated that security was a legitimate need for CPR, based on past incidents. Second, it concluded that the cameras would deter future theft, vandalism, and trespassing, and would also be a valuable tool in investigation if deterrence failed, and that on the balance of probabilities the evidence indicated they were effective in meeting CPR’s security needs. On the third factor, the Federal Court found that the loss of privacy was minimal, because the “collection of personal

---

697 Ibid.
698 Eastmond, supra note 675.
699 Ibid at paras 127, 131.
700 Ibid at para 174.
701 Ibid at para 177
702 Ibid at paras 178, 179.
information [was] not surreptitious... [and] not continuous”, and also because the images were “never viewed unless there [was] a triggering event.” Finally, it considered that the alternatives (such as fencing around the entire yard or the hiring of security personnel) were either not cost effective or would disrupt CPR’s operations, and thus given the low loss of privacy, the fourth factor could be answered in the negative. Nonetheless, while rejecting the determination of the OPC, the Federal Court in *Eastmond* approved the four-part framework, and the OPC has subsequently adopted it as not only a test for the reasonableness of an information practice in the context of visual surveillance, but more broadly as well. In the following section, I consider the application of the *Eastmond* test to the operation of geo-immersive technologies, and suggest that they can be considered presumptively ‘reasonable’, though the test may need elaboration in certain areas.

*Step 1: Demonstrably necessary to meet a specific need*

The first step under *Eastmond* is a determination of whether the measure in question is demonstrably necessary to meet a specific need; if the need cannot be articulated sufficiently or if the practice cannot be shown to be ‘demonstrably necessary’ in meeting it, then any collection, use, or disclosure would seem to instantly fail the reasonable purposes requirement. In general, the interpretations of what counts as a ‘specific need’ have been quite broad – the OPC’s contention in the CPR case finding that security was not a specific need but rather merely a ‘potential’ one given the circumstances, *supra*, appears to have been a relative outlier. There have been no subsequent OPC case findings that have applied the *Eastmond* framework but

---

703 *Ibid* at paras 176, 188.
704 *Ibid* at para 182.
have found a stated need *not* to meet this threshold of specificity. There are apparent limits however – consider the OPC’s own Report regarding Google’s accidental collection of Wi-Fi data through the use of its Street View cars that I earlier referenced.\textsuperscript{706} The Report concluded that the “nature of [Google’s] operations – a secret and sweeping collection of data” violated s. 5(3), since it was “impossible to conceive that a reasonable person would have considered such collection appropriate in the circumstances”.\textsuperscript{707} Admittedly, the OPC did not make reference to the *Eastmond* framework, though they explicitly stated that that the collection was ‘inappropriate’ under s. 5(3). It is possible that may have been simply because the information practice in question was so clearly unreasonable by any determination (the secretive collection of personal information including emails, financial records, computer passwords, etc.) that any detailed explanation was unnecessary.\textsuperscript{708}

Unlike in the Wi-Fi case, however, it is reasonable to conclude that the commercial service provider’s collection of personal information in the context of geo-immersive surveillance meets this threshold. Even though it was the operation of the same Street View cars that led to the inappropriate collection of private information in the Wi-Fi case, there is no suggestion that the OPC views the photography of public spaces as ‘inappropriate’ on its face. The ‘need’ is the operation of the geo-immersive service, and the collection of personal information in the course of doing so is ‘demonstrably necessary’, since there is currently no plausible way of operating

\textsuperscript{707} *Ibid* at para 21.
\textsuperscript{708} *Ibid* at para 18.
the service without collaterally gathering the personal information of those who happen to be in the area. 709

Step 2: Effectiveness in Meeting the Need

In many examples, the second step of the framework (which asks whether or not the measures taken are likely to be effective in meeting the defined need) is a relatively straightforward evidentiary question. For instance, are the security cameras in fact effective in increasing security (or are they likely to be), 710 or does the collection of thumbprints in fact assure the authenticity of test scores used for admittance to law schools? 711 In such cases, it is relatively easy to determine whether or not the information practices are in fact effective. Since the question can be asked “is this information practice in fact meeting the stated need?” and the answer will vary given the evidence, it is a useful step in determining whether or not an impugned information practice is in fact ‘appropriate’ under s. 5(3). Here, geo-immersive providers appear to meet the necessary threshold – the collection of personal information that occurs through the imaging of the cityscapes is part of the successful photographing of public spaces that is necessary to the operation of geo-immersive websites.

Step 3: Proportionality

At the third step, the Eastmond test focuses on the issue of proportionality – a consideration of the harm suffered by the individual as a result of the impugned information practice versus the benefit gained. In Eastmond, for instance, the Federal Court concluded that the static nature of

709 There is also the possibility that the service providers in fact desire the personal information they gather, not necessarily in order to identify individuals, but rather to make the ‘explorable worlds’ appear more reflective of their day-to-day state.
710 Eastmond, supra note 675.
711 PIPEDA Case Summary #2008-389, supra note 705.
the images generated by the security cameras and the irregular intervals at which they would be viewed meant that there was a relatively low infringement of privacy, and thus proportionality was achieved between it and the benefits of increased security. It is relatively easy to ask proportionality questions about the benefit of improved security in a parking lot or more assured authenticity of test-takers versus the privacy loss caused by the relevant collection of personal information in each case, largely because there are conventionally accepted levels of appropriate security and appropriate identity protection. The question here then is what benefits do geo-immersive technologies bring, and are they proportional to the privacy losses caused? Service providers clearly believe that there will be significant commercial benefit to these maps at some point. However, I have also argued that geo-immersive technologies do bring public benefits (again, by ‘public’ here I mean broadly accessible to the population as a whole, even if they are privately run or commercially operated). I would argue that laid out in the fashion I have described, the privacy losses caused by geo-immersive technologies as they are currently run appear proportional to the benefits gained. I have suggested that while geo-immersive technologies do threaten to reduce the ability of the individual to calculate their exposure, for the moment this occurs rather infrequently. It is the potential for significantly more frequent photography thanks to a lack of effective regulation that concerns me. Thus, should the intensity of the surveillance greatly increase, then this calculation of proportionality would necessarily also change. For instance, more frequent image capture or the use of constant live video rather than irregular photography would be considered a much more serious privacy loss, and therefore would likely tilt the proportionality question in favour of ‘unreasonable’. This is also the case, for instance, if we consider the application of this proposed test to the Google Wi-
Fi collection incident discussed earlier. Even though the OPC declined to apply *Eastmond*, it stands to reason that had Google been able to identify a legitimate need for the information, it would not have been proportional to the harm caused. In that situation, the information collected was often highly sensitive, and could have led to the creation of highly detailed dossiers about the private life of those whose information was captured. Those harms were clearly disproportionate to the minimal benefits to collecting the information; it would have been impossible to justify that privacy loss, and that practice would surely be classed as ‘unreasonable’ under s. 5(3).

*Step 4 – Is there a less privacy-invasive way of achieving the same goal?*

It can always be asked whether or not there is a less privacy invasive way of achieving the same goal, even if that goal can only be defined as commercial benefit or profit. At the moment, it appears as though geo-immersive service providers are using industry ‘best practices’ for the electronic blurring of faces, though as I have argued those current standards are inadequate to the task. In theory, the providers could also limit the amount of personal information they gather by conducting their operations in the early hours of the morning, or by requiring the camera operators to halt their operations whenever individuals are within the vicinity. It does not appear plausible to require camera operators to turn off the cameras whenever an individual is in the field of view – it would seem to make mapping urban areas virtually impossible. However, it may be necessary to draw a distinction between the ‘collecting’ and ‘distributing’ information practices that together make up the geo-immersive information practice as a whole. While it seems reasonable to say that there is no less privacy-invasive of currently *collecting* the personal information, I will nonetheless argue in the next section that a more rigorous
application of technical safeguards and investments in more effective blurring techniques ought to be mandated by the OPC when it comes to the subsequent distribution of that information.

In general, though, my conclusion is that (as they currently operate) geo-immersive technologies ought to be classed as ‘reasonable’ within the meaning of s. 5(3) of PIPEDA. I have argued above that the operation of geo-immersive technologies appears to implicate the provisions of PIPEDA – they collect, use, or disclose personal information, and do not obviously fall outside the reasonableness standard established by Eastmond. This means, then, that the service providers ought to be required to meet the necessary standards outlined in Schedule 1 of PIPEDA. The Schedule 1 principles can be traced back to the ‘fair information’ principles first enunciated in the OECD Privacy Guidelines. Those guidelines were introduced to Canada prior to the enactment of PIPEDA through the adoption in 1996 by the Canadian Standards Association of the “Model Code for the Protection of Personal Information.” While a voluntary industry charter rather than a binding law, the Model Code also referenced the fair information principles and ultimately became the document upon which the Schedule 1 protections in PIPEDA were based. In the following section, I intend to argue that existing service providers appear non-compliant in three key areas under these principles: knowledge and consent (under principle 4.3), limiting collection (under principle 4.4), and choosing appropriate safeguards (under principle 4.7). The most important of these, in my view, is the knowledge and consent requirement, and it is that which I will first consider.

712 Attached as Appendix 1
713 Attached as Appendix 2.
Knowledge & Consent

Clause 4.3 outlines the key elements of the informed consent requirement:

4.3 The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

4.3.1 Consent is required for the collection of personal information and the subsequent use or disclosure of this information.

4.3.4 The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

4.3.5 In obtaining consent, the reasonable expectations of the individual are also relevant.

4.3.6 The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive.  

Without informed consent an organization cannot collect, use or disclose the personal information of an identifiable individual. Now, it is obvious that the operators of geo-immersive surveillance are not seeking or receiving express consent from individuals whose personal information they capture via the photography of public spaces and then subsequently distribute through the online services. To remain in compliance with PIPEDA then, they must have either received implied consent of the individuals whose information they process, or be able to fit within the exceptions to the consent requirements – Clause 4.3 notes that in certain

---

714 PIPEDA, Schedule 1, Clause 4.3.
715 See for instance Englander v Telus, 2004 FCA 387.
circumstances consent might be ‘inappropriate’, and s. 7 of PIPEDA details when this will be the case.\(^{716}\) None of the exceptions to the consent requirement appear relevant to the operation of geo-immersive possibilities, save possibly where the personal information in question is publicly available and of the type specified by the regulations. However, it is not applicable to simply any personal information that can be drawn from the public realm, but rather only to specific classes of information defined in the relevant Regulation, which would appear to foreclose any reliance upon it by a geo-immersive service provider.\(^{717}\) Moreover, regardless of the category in which the information is claimed to be residing, for the exception to be applicable the information must have actually been collected from the specified source before it can be used or disclosed without the consent or knowledge of the individual to which it refers. It is not sufficient for an organization to argue that it was possible they could have gathered the information from a publicly available source identified in the Regulation, if in fact they acquired

---

\(^{716}\) PIPEDA, s 7(1)-(3). Speaking in general terms, the exceptions for collection without consent include where it is in the interests of the individual and consent cannot be obtained, where requesting consent would hamper the investigation of a breach of an agreement or law, where the use is solely for journalistic, artistic, or literary purposes, where the information is publicly available, and e) where it is collected for the purposes of making a disclosure required by law. Interestingly, s 7(1)(c) (the clause regarding journalistic, artistic, or literary purposes) appears to be redundant, given that the existence of the inapplicability of the entire Act in such circumstances. This is probably a function of the choice to directly adopt the CSA Model Code into PIPEDA, instead of crafting an entirely new document aimed at protecting the same principles. The exceptions for use also include an investigation into the contravention of law, where an emergency requires it, where it is used for statistical or scholarly research, or where it was publicly available. The exceptions for disclosure without knowledge and consent include where the disclosure is made to a lawyer representing the organization, where it is for the purpose of collecting a debt, where it is required to comply with a legal order, where it is made to a government authority for certain defined purposes, where it is necessary due to an emergency, where it is made for statistical or scholarly research, where it is made to a conservation or archival organization, where it is made twenty years after the death of the individual concerned, or where it is otherwise required by law.

\(^{717}\) The Regulations Specifying Publicly Available Information, SOR/2001-7 include the following classes of publicly available information. An individual’s name, address, and telephone number when they have voluntarily chosen to have it in a telephone directory; an individual’s name, title, address, and telephone number that appears in a business directory, so long as the collection, use, or disclosure relates to the reason the business directory exists; any personal information that appears in a registry as the result of being collected by a statutory authority, so long as the collection, use, or disclosure relates to the purpose for which the information is in the registry; any personal information that appears in the judicial record (or that of a quasi-judicial body), so long as the collection, use, or disclosure relates to the reason the information is in the record; any personal information that appears in a publication, including a magazine, book, or newspaper, in printed or electronic form, so long as the individual voluntarily provided that information initially.
it by another means. It is also insufficient to argue that once the information has been legitimately disclosed through one of the publicly available exception categories, that no further consent is needed from the individual in question for further uses or disclosures. Regardless, the collection of personal information via surveillance of public spaces does not fit within the specified Regulations, and the OPC has typically found that where individuals are going about their daily business on a street, their consent is still required for the collection of their personal information via video cameras, despite the public nature of the space. Indeed, the OPC has directly confirmed that is the case in the context of geo-immersive surveillance:

If an organization takes a photograph of an individual in a public place for a commercial purpose—for example, when a company, in the course of photographing a streetscape, captures an identifiable image of a person and that image is uploaded onto the Internet for a commercial reason—Canadian privacy law still applies. One of the key protections is that people should know when their image is being taken for commercial reasons and what the image will be used for. Their consent is also needed.

The question turns, then, to one about the form that consent must take—express or implied. Clearly, the operators and providers of those technologies are not seeking (and realistically cannot seek) the express consent of every single individual who is imaged by their cameras; the consent must therefore be implied. Typically, in order to be able to rely on the implied consent of the individuals whose information organizations seek to collect, use, or disclose, two

---


719 See for example PIPEDA Case Summary #2010-004, “Manager’s remark reveals employee’s salary—consent was necessary despite existing public disclosure requirement”, available online, http://www.priv.gc.ca/cf-dc/2010/2010_004_0726_e.cfm, last accessed Nov 15, 2011, in which the OPC found that where an individual’s salary was publicly disclosed through audited financial statements available at a public library, separate consent from the individual was required before it could legitimately be disclosed in other contexts (in that circumstance, the employee’s supervisor had told the employee’s co-workers his salary as part of a complaint about his work performance.)

720 PIPEDA Case Summary #2001-1, supra note 652.

requirements must be met – that the information in question be ‘less sensitive’, and that the individuals in question have received ‘notice’.722 This, indeed, appears to be the approach thus far apparently723 taken by OPC to geo-immersive surveillance; the Assistant Commissioner testified with regard to geo-immersive imagery that the OPC considers the imagery generated not sensitive and the service providers can rely on the implied consent of people photographed, so long as they have given notification in the form of ‘outreach’:

[T]he nature of the information collected is not especially sensitive and that companies can rely on implied consent, provided they give reasonable notification to the public in the form of outreach.724

Interestingly, this also appears to prove Austin’s argument that a regime of reasonableness and notice provides no less a level of privacy under PIPEDA than does a regime of reasonableness, notice, and consent.725 She argues that past case findings by the OPC suggest that where purposes are found to be reasonable and the individual in question has been notified, then “a finding of implied consent follows.”726 The Assistant Commissioner’s testimony suggests this is precisely the case – despite arguing that individual consent is necessary for street photography, the requirement appears to actually be doing little substantive work, and has in effect been subsumed under the question of notice.

722 PIPEDA clause 4.3.6.
723 No official finding has been made by the OPC with regard to the operation of geo-immersive technologies, and so I am relying on their issuance of relevant guidelines and comments made before Parliamentary Committees when attempting to glean its approach.
724 Testimony of Elizabeth Denham, before the Standing Committee on Access to Information, Privacy, and Ethics, Oct. 22, 2009, evidence, ETHI, No. 032, 2nd Session, 40th Parliament, at 2. I contend later in this Chapter that despite this statement, the OPC has not really required the application of any of the relevant provisions of Schedule 1 to geo-immersive imagery, not even this “reasonable notification” as identified by the Assistant Commissioner.
726 Ibid.
In the following sections, then, I consider the validity of the OPC’s decision to rely upon implied consent in the context of public street photography. I conclude that while it is unreasonable to presume that all personal information gleaned from public spaces through geo-immersive technologies is of the ‘less sensitive’ variety, I do accept that the majority of such information is likely non-sensitive. However, I argue that the notice provided by providers of those technologies is woefully inadequate, and that low sensitivity does not eliminate the need for notice but rather allows for implied consent where there is sufficient notice. As a result, the OPC’s current approach to the operation of geo-immersive technologies is not justified by a legal analysis based upon implied consent through notice of the collection, use, and disclosure of non-sensitive information.

The Sensitivity Question

As I have indicated, under PIPEDA it is stated that organizations engaged in the collection, use, or disclosure of personal information for commercial purposes can “generally” rely upon ‘implied consent’ where the information in question is ‘less sensitive’.\(^\text{727}\) Distinguishing when personal information is sensitive and when it is not is, however, not always clear-cut. On the one hand, certain kinds of personal information are considered to always be sensitive – health information and income information, for instance.\(^\text{728}\) Sensitive information can go beyond those categories, however, depending on context. The example given in the text of PIPEDA itself is that subscriber information for a magazine is typically not sensitive, but if it were a particular kind of magazine aimed at certain special interests, then such information might be.\(^\text{729}\) Under

\(^{727}\) PIPEDA, clause 4.3.6.
\(^{728}\) PIPEDA, clause 4.3.4.
\(^{729}\) PIPEDA, clause 4.3.4.
the case findings, these basic categories and related contextualization have been affirmed.
While medical information, financial details including social insurance numbers, and purchasing habits and preferences have all been deemed sensitive, mere names and addresses of individuals both have and have not been found as such, depending on the context in which they are collected. For instance, names and addresses have been declared sensitive when connected to a survey with other questions regarding income levels, but not sensitive when used for secondary marketing purposes by a retail bank.

The question of sensitivity, then, is largely one of context. The Federal Court, for instance, has concluded correspondence might be ‘sensitive’ – in the context of a labour dispute, the court found there to be a meaningful distinction between general correspondence from an employer to a unionized employee and correspondence between the same that contained sensitive information; the former could be disclosed to the union without the explicit consent of the employee, while the latter could not. While not specifically stated by the Federal Court, it seems likely that the general correspondence would have been considered ‘personal

---

information’, given that it clearly identified the employee and the existence of her complaints about harassment by a superior; it was therefore only its lack of sensitivity that allowed consent to be implied. Because the sensitivity of personal information has to be determined on a contextual basis, there can be no exhaustive list of personal information that is sensitive and a companion list of information that is not. The Federal Court has also indicated that the subjective feelings of the individual are also relevant to a determination of sensitivity.\footnote{Randall, supra note 656.}

In \textit{Randall}, the applicant had complained that the release of this information to his employer in conjunction with a corporate fitness membership was done without his explicit consent. The OPC initially found that the fitness centre could have relied upon the applicant’s implied consent if the applicant had been provided notice of the possible disclosure at the time he signed up for the gym membership. Since that notice was not provided, express consent was required. Since express consent had not been sought, PIPEDA had been violated. The matter was ultimately brought to the Federal Court, which agreed that the fitness centre had indeed “disclosed personal information relating to the applicant’s fitness centre usage without his consent and thereby violated his privacy.”\footnote{Ibid at para 36.} The Court concluded, however, that while information about attendance at a fitness centre was “at the lower end of the scale of sensitivity, viewed objectively”\footnote{Ibid at para 42.}, \textit{subjectively} the information disclosed was sensitive, because the information was “being disclosed to [the applicant’s] work colleagues at a staff meeting and encouraged rivalry… that made him uncomfortable.”\footnote{Ibid at para 43.} This led the Federal Court to conclude
that despite the objectively low sensitivity of the information, the fitness centre could not
legitimately rely upon implied consent and they were therefore in breach of PIPEDA.\footnote{Ibid. No damages were awarded, however, because the breach was not considered ‘egregious’.
\footnote{In a dispute regarding the placement of video surveillance cameras at a bus terminal the OPC suggested that “the
personal information being collected [was] not very sensitive”, see PIPEDA Case Summary #2009-001, supra note 679.}}

With this in mind, where does the imagery collected and disclosed by geo-immersive
surveillance fall on this scale of sensitivity? In only one past OPC finding was imagery of
individuals found to fall into the ‘less sensitive’ category.\footnote{Ibid. No damages were awarded, however, because the breach was not considered ‘egregious’.
\footnote{In a dispute regarding the placement of video surveillance cameras at a bus terminal the OPC suggested that “the
personal information being collected [was] not very sensitive”, see PIPEDA Case Summary #2009-001, supra note 679.}} In other findings related to
captured imagery, the OPC did not address the sensitivity question, but rather just considered to
be a form of personal information and the analysis proceeds from there. There is therefore little
material from which generate a predictive hypothesis. However, as noted the OPC has stated
before the relevant Standing Committee that it sees the kinds of images generated by geo-
immersive technologies like Google Street View and Canpages as ‘less sensitive’, and I agree
that the majority of the kinds of information generated by geo-immersive technologies will be of
the less-sensitive variety. If one takes the holding of Randall into account, however, then one
must accept that the sensitivity of information is a contextual and at least partially subjective
question; one cannot say that imagery of individuals in public is inherently ‘non-sensitive’. The
possibility certainly exists that more sensitive information could be captured in such images –
for instance, an individual entering or leaving an abortion clinic, or a particular religious
institution. In both cases, reasonable inferences could be drawn (the person was accessing
certain healthcare services or belongs to a certain religious denomination) that typically would
be thought of as ‘sensitive’. The fact that these inferences were drawn from public behaviour
does not make them less sensitive, either as a matter of logic or as a matter of legal analysis based on the existing OPC case findings. It is risky, therefore, to argue that as a matter of principle geo-immersive technologies capture only non-sensitive information. At best, one can argue that it collects predominantly non-sensitive imagery. But even if one accepts that the images are predominantly (or even entirely, for the sake of argument) non-sensitive and therefore reliance can be made on implied consent, sufficient notice to the individual about the information practice at issue is still required.

The Notice Question

Reliance on implied consent can only be made where there are “circumstances [that] indicate that an individual has a certain understanding, knowledge, or acceptance, or certain information has been brought to the attention of an individual.”742 There are effectively then two ways knowledge of the information practice can be imputed – pre-existing acceptance of the practice or explicit notice drawing attention to the practice. This means that under certain circumstances, the requirements for valid implied consent can be met even without notice, because the individual can be presumed to already have the necessary awareness. However, the OPC appears to have already rejected this approach in the context of geo-immersive technologies. In her testimony before the Standing Committee the Assistant Commissioner discussed the need for public ‘outreach’;743 if individuals were considered to have a pre-existing awareness regarding commercial street photography, such outreach would presumably not be necessary.

743 Testimony of the Assistant Commissioner, supra note 724.
The OPC’s own case findings (while not binding) also suggest that reliance on such pre-existing acceptance is only valid in the context of an *already existing* information relationship between the individual and the organization. In other words, it is only where an initial valid consent (be it explicit or implied) to the collection, use, or disclosure of personal information exists that the reasonable expectations of the individual may then eliminate the need for subsequent notice of unspecified additional collections, uses, or disclosures.\(^{744}\) I am unaware of any OPC case findings that suggest the reasonable expectations of the individual as understood under clause 4.3.5 can do away with the need for notice entirely for the *initial* consent to the collection, use, or disclosure of an individual’s personal information by an organization. This suggests that clause 4.3.5 does not allow the reasonable expectations of the individual to directly guide when and under which circumstances organizations can collect, use, or distribute the personal information of those individuals *without* their consent, but rather guides only the *form* of that consent, and it is only under very limited scenarios that this form will not require notice in one form or another. The reasonable expectations clause, while certainly relevant to the form

---

\(^{744}\) See for instance PIPEDA Case Summary #2001-23, “Employee objects to employer’s use of bank account number on pay statement”, online, [http://www.priv.gc.ca/cf-de/2001/cf-de_011105_01_e.cfm](http://www.priv.gc.ca/cf-de/2001/cf-de_011105_01_e.cfm), last accessed Nov 24, 2011, in which the OPC concluded that where an individual had consented to the direct deposit of their paycheque, they had also implicitly consented to the appearance of account-related transit numbers on their pay statements, even though they were not given direct notice that those transit numbers would appear. See also PIPEDA Case Summary #2007-382, “Former employer discloses drug testing information”, online, [http://www.priv.gc.ca/cf-de/2007/382_20070727_e.cfm](http://www.priv.gc.ca/cf-de/2007/382_20070727_e.cfm), last accessed Nov 25, 2011, in which when dealing with a complaint from an individual whose previous employer had sent a negative job evaluation to a prospective employer, the OPC concluded that initial *express* consent from the individual to the prospective employer calling the previous employer for a reference included *implied* consent to that previous employer offering a negative evaluation. Most recently see PIPEDA Case Summary #2009-008, *supra* note 632, in which the OPC suggested that the reasonable expectations of the user under clause 4.3.5 were relevant in relation to the default settings that Facebook offers to protect user privacy. The OPC found that users were required to provide an initial explicit consent to the terms of service of the website, which incorporated a reference to a set of default privacy settings for personal information shared with Facebook; the issue of reasonable expectations under clause 4.3.5, therefore, related to the content of these defaults – again, a secondary rather than initial consent.
consent is required to take, does not therefore appear to provide a means for a complete end-run around the core requirement of that consent – that it be informed – when it is consent to the information practice commencing. Geo-immersive technology providers should not be able to argue, therefore, that no notice is required to establish implied consent on the part of individuals appearing in the images, because the consent at issue is the initial and primary one that begins the relationship between the individual and the organization. As a matter of course, the OPC and the courts have both long recognized the importance of notice as a component of implied consent in cases of visual surveillance. This means that in order for geo-immersive technology providers to rely upon implied consent under PIPEDA, they must still provide adequate notice. Are they so doing?

As I have noted, the OPC has deemed that ‘outreach’ by geo-immersive technology providers is sufficient notice. Figures 23 and 24 are examples of the current form of this ‘outreach’ undertaken by Google (again, I am singling out Google as the paradigmatic example and market leader, but there are no service providers that currently provide more detailed notice). Both examples are screen captures of the information provided by Google to visitors to its website regarding Street View operations in Canada and the United States, respectively, on Nov. 22, 2011; the lack of helpful information for residents wishing to avoid being photographed is apparent.

Note: because I am referring here to notice as an element of ‘implied consent’, this statement does not refer to the cases of surreptitious video surveillance of individuals suspected of breaking a contract or defrauding an insurance company. Under PIPEDA, consent is not necessary for the collection of personal information in such cases, and therefore notice is not a relevant component, supra note 716.

As the above images demonstrate, no specific notice is given of the exact dates or times of when the photography will start or commence, or the order in which the city will be photographed, nor is there any option for users to sign up for automatic notifications of when their city will be photographed. Large areas may have cars *somewhere* in them, with no hours or dates of expected operation or termination. In order to receive this ‘notice’ in a timely fashion, an
individual would have to check the Google Street View website daily in order to discover whether or not camera-bearing cars are roaming their city on that particular day.

This outreach, considered an acceptable form of notice by the OPC, is therefore nothing more than token. And yet, the OPC has previously indicated that where only token efforts are made to notify and seek consent from those potentially affected, the requirements of PIPEDA are not satisfied.747 In the context of surveillance, the OPC has typically required clarity in signage or communication that makes subjects of surveillance aware of the existence and location of cameras, and their purpose. In workplace disputes, for instance, the OPC has noted with approval an employer’s decision to notify its employees of the presence of surveillance cameras and to issue regular bulletins about their operation and purpose.748 Outside the workplace, the OPC has required that landlords notify tenants of interior photography of their apartments.749 In considering the installation of security cameras in a bar, the OPC found while initially no consent had been given to the consequent collection of personal information, this was rectified by the presence of warning signs at the entrance of the bar (though finding ultimately that the collection was not a ‘reasonable purpose’ and thus violated s.5 (3) of PIPEDA.750 With regard to surveillance cameras at a bus station that recorded both employees and non-employees, the

748 See for instance PIPEDA Case Summary #2004-264, supra note 677, and PIPEDA Case Summary #2006-351, supra note 680. See also Eastmond, supra note 675, in which the Federal Court noted the clear presence of ‘warning signs’ regarding the installation of video cameras as one of the factors that led it to dismiss an application for enforcement of an OPC finding (at para 191). (As a caveat, the issue of implied consent “was raised but not really argued” in Eastmond; the original OPC finding had related to whether or not the surveillance in question was a ‘reasonable purpose’ within the meaning of s 5(3), and also failed to consider the issue of consent. Nonetheless, the importance of sufficient notice was made apparent by the OPC and the Federal Court.)
749 PIPEDA Case Summary #2006-349, supra note 651.
750 PIPEDA Case Summary #2008-396, supra note 671.
OPC found that signs alerting to the presence of the cameras were “clearly visible”, and thus implied consent could be relied upon.\textsuperscript{751} Most recently, the OPC criticized a grocery store for failing to have adequate signage notifying individuals that they were under video surveillance, concluding that “a monitor at an entranceway and cameras hanging high overhead, by themselves, do not provide clear and sufficient notice to patrons that a video surveillance system is in use.”\textsuperscript{752} As a result, patrons were not deemed to have consented to the collection of their information.

Together, these cases indicate that for notice to be considered effective, it has to have had a good chance of actually being received by the individuals to whom it pertains. Signage must be clear, noticeable, and posted at any entrance to where surveillance is being undertaken. None of these factors are met by the current form of outreach undertaken by geo-immersive technology providers in Canada. The OPC’s decision to rely on such outreach as acceptable can only be based on their contention that the information gathered is non-sensitive, and that individuals do not have a reasonable expectation of privacy in public. Yet, the bifurcated nature of the surveillance infrastructure that characterizes these technologies in fact demands a more rigorous interpretation of the notice requirement, precisely because the consequences can be so great, even if the majority of information gathered does in fact fall into a ‘less sensitive’ category.

Limiting Collection

\textsuperscript{751} PIPEDA Case Summary #2009-001, supra note 679.
\textsuperscript{752} PIPEDA Case Summary #2011-003, supra note 652.
Clause 4.4 outlines the requirements organizations must meet with regards to the collection of information:

4.4 The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

4.4.1 Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle.

In this section, I want to focus on clause 4.4.1 – that organizations shall not collect personal information indiscriminately, which has been interpreted as meaning the purpose of the collection is uncertain in scope, or “open-ended” without reason, such as when a bank asks for a social insurance number but does not fully explain the reason why.\(^753\) Primarily, however, the OPC has considered ‘indiscriminate’ to mean unnecessary, reading it largely in conjunction with 4.4 – for instance, the request by a telecommunications company for an individual’s social insurance number as part of her application for an Internet connection was found by the Commissioner to be “indiscriminate” because it was “not necessary to fulfil explicitly specified and legitimate purposes.”\(^754\) This was also the approach taken in a case regarding the collection of information about the owner of car brought into a repair shop for a routine oil change – the Commissioner indicated that clause 4.4.1 meant that organizations “must limit their collections to amounts and types of information necessary for the purpose at hand.”\(^755\)

\(^753\) See PIPEDA Case Summary #2003-203, \textit{supra} note 731.
If the purpose of the geo-immersive programme is to generate maps, clause 4.4.1 means only the information necessary to generate those maps ought to be collected. Since the collection of geo-immersive information can occur repeatedly, at any time, even after the initial map has been created, such collection of personal information via geo-immersive technologies can be seen as ‘indiscriminate’. While such regular collection is not yet a feature of typical geo-immersive providers, I argued in Chapter 2 competitive pressures will likely increase both the quality and frequency with which images are taken, as companies seek to differentiate their offerings. I will therefore argue in Chapter 8 that reinvigoration of clause 4.4.1 in a fashion that looks not only to a link between the kind of information collected and the purpose of the information practice but also to the frequency with which it is collected may serve to be a fruitful means of regulating the growth of geo-immersive surveillance.

Safeguards

Clause 4.7 details the requirements organizations must fulfil under PIPEDA with regard to protecting the data they have collected:

4.7.1 The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2 The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection.
These provisions are generally aimed ensuring organizations adopt particular steps to ensure personal information they have collected does not fall into the wrong hands, or if it does, that appropriate protections are in place to minimize the damage. It also includes actual execution of those policies – it is not enough for policy to simply exist if the organization fails to implement it properly. For instance, a bank was deemed to have violated 4.7.1 by failing to properly execute its stated security policies and procedures regarding client information after client files sent through the mail on a portable disk drive went missing.\textsuperscript{756} Even where users have consented to the sharing of their personal information, safeguards under this clause are necessary to ensure what is shared is the minimum necessary to fulfil the identified purposes to which the user consented. Regarding the provision by Facebook of the personal information of its users to application developers, for instance, the OPC found the social networking company in breach of 4.7 because it did “not have adequate safeguards in place to prevent unauthorized access to users’ personal information.”\textsuperscript{757}

The safeguards principle is also relevant in the case of surveillance. The OPC has found that where video surveillance imagery is made available online, strong security measures are required to ensure it is viewable only by the intended parties. This conclusion was reached in the context of a webcam installed in a day-care, allowing parents to view their children through their workplace computers. The OPC concluded that the day-care was “obliged to take reasonable steps to ensure that parents do not use the video stream captured by the webcam for


unrelated and unauthorized purposes (for example, recording and further disclosing information viewed on the Web.”\textsuperscript{758} The day-care was found to have met its obligations when it developed a privacy policy, changed its software to prevent easy recording by parents, and password-protected the video stream so that only parents with children registered at the day-care could access the stream.

These case findings indicate that under clause 4.7, geo-immersive technology providers ought to implement safeguards to ensure that the personal information they collect does not fall into the hands of others. The techniques by which they do this are two-fold, and I discussed them in greater detail in Chapter 2. To review, all geo-immersive technology providers attempt to digitally blur faces and licence plates, though as I indicated this is far from a fool proof method and still allows for identification of individuals in many circumstances. Second, service providers allow for individuals captured in images to request ‘take downs’ of the images if the blurring has failed, or if they reveal some particularly objectionable activity. However, geo-immersive technology providers have made no effort, for instance, to develop techniques of preventing end users from copying the images so that they may be re-shared in a viral fashion, even if the original has been taken down. The bifurcation of the surveillance infrastructure means that stronger, not weaker technical safeguards ought to be implemented, and I will argue for these in Chapter 8.

It is possible, of course, that geo-immersive technology providers may argue that existing
techniques, imperfect as they are, are “industry standard” or otherwise represent best efforts. I
would note, however, that where technical measures to safeguard the information are not
feasible, then according to the OPC enhanced notification of that fact is required. For instance,
in a complaint about an airline ticketer, unmasked credit card numbers were printed on paper
tickets. The OPC concluded that while e-tickets could show masked credit card numbers, the
technology did not exist to mask numbers on the paper ones; while this violated 4.7, the solution
settled on by the OPC was to “inform customers at the time of purchase that their full credit card
number and expiry date will appear on the paper ticket and [that] e-tickets, which mask all but
the last four digits of the credit card number, are available.” Admittedly this is a somewhat
confusing approach by the OPC, in that they effectively deemed an organization in violation of
clause 4.7 even though there were no means of improving the safeguards. Nonetheless, it does
appear as though if there are limitations to the kinds of safeguards that are available, then the
OPC will at a minimum require enhanced levels of notice to subjects of information practices
informing them of that possibility. As I have shown in the section on ‘notice’, geo-immersive
providers are certainly not providing particularly stringent notice to people who may be subject
to their cameras. Regardless of the OPC’s approach to the interaction between clause 4.7 and
4.3, however, I will argue in Chapter 8 that investing in improved technical safeguards for geo-
immersive imagery may go a significant distance to reducing the possibility of social harms
arising through their widespread operation.

759 PIPEDA Case Summary #2007-386, “Credit card information printed on paper airline tickets not a proper
safeguard; transfer of personal information to travel wholesaler questioned”, http://www.priv.gc.ca/cf-
Summary

I have argued in this chapter that PIPEDA appears applicable to the kinds of information practices associated with geo-immersive technologies – I have suggested that the practices appear presumptively reasonable under the *Eastmond* standard, and they meet the requirements that trigger the application of the substantive requirements under Schedule 1. However, I have also concluded that the OPC is not rigorously enforcing those requirements. In the next chapter then, I want to suggest that if one considers the “privacy interests” at play in PIPEDA to be of the kind represented by the relational approach I advocated in Chapter 4, then it may be reinvigorated in a way that serves to effectively regulate geo-immersive technologies so that the potential social risks I have identified do not come to pass. In other words, an approach grounded in relational privacy may justify a more stringent application of the fair information principles in the context of geo-immersive technologies.
Chapter 8: Reinvigoration of PIPEDA Through Relational Privacy

I argued in the last chapter that it appears that PIPEDA is applicable to the kinds of information practices associated with geo-immersive technologies, the current implementation of the substantive protections under Schedule is inadequate, and therefore the current use of geo-immersive technologies is *not* in compliance with at least some of those requirements. In this Chapter, then, I will advance a more robust implementation of those requirements, justified by reference to the ideas of relational privacy. I will argue that a more rigorous application of Schedule 1 in a fashion that is reflective of the commitments of relational privacy is likely to have the effect of significantly reducing the potential that the systemic harms I have identified will come to pass, and therefore can serve as an effective regulatory framework.

A More Robust Application of Schedule 1

Schedule 1 to PIPEDA implements the well-known fair information principles that have globally influenced the development of data protection legislation. While some scholars have criticized the use of the fair information principles as a means of regulating surveillance, I suggested in the last Chapter that they *are* in fact adequate to the task of limiting the evolution of public street surveillance. Where the surveillance infrastructure is bifurcated, if properly implemented those principles can have the effect of significantly limiting the amount and kind of imagery that is collected at the first stage, thus greatly limiting the scope the second stage has for scrutiny and possible influence on behaviour. I also argued that the current application of these principles by the OPC in the context of public street surveillance is inadequate. Therefore, a more rigorous interpretation is necessary to successfully limit the further emergence of the surveillant infrastructure I have identified as being associated with geo-immersive technologies.
I earlier suggested that privacy is best understood as an on going process which the individual seeks to negotiate their exposure in a manner that helps them negotiate their relationship and existence within the broader community. I drew upon the work of Palen & Dourish to suggest that this is a dialectical process features at least three boundaries – one that related to the disclosure of information between one’s personal life and public face, one that related to identity formation at the intersection of the self and the other, and one that related to information disclosure across different points in time. I also noted that these boundaries were characterized by different levels of permeability. Petronio suggests that:

The boundary walls may be thick or thin, influencing the access to or protection of private information. When the walls are thick, the boundaries are tightly controlled affecting the depth, breadth, and the amount of private information that is communicated. When the walls are thin, the boundaries are loosely held and there is more permeability regarding these issues.

I want to suggest in this Chapter that the substantive Schedule 1 protections can be interpreted in fashion that would achieve the ‘correct’ level of permeability in the context of regulating geo-immersive surveillance, when taking into consideration the benefits of the programme along with the associated potential risks. I argue, therefore, that PIPEDA can in fact incorporate a dialectic account of privacy. I intend to show that the requirements of Schedule 1 can be calibrated in a fashion that better preserves the ability of individuals to control their exposure in public space whilst not entirely preventing organizations from being able to gather personal information from that space. In the parlance of the dialectic accounts, this sets the permeability of the boundaries at the right level – they are not too thick (banning all collections of personal information in public space without the express consent of every individual present), nor are

---

760 See Chapter 5, pp. 147-150.
761 See Chapter 5, p. 145.
they too thin (allowing unlimited and unrestricted collections of personal information from public space). This calibration remains consistent with the nature of PIPEDA as a legislative tool that is premised on balancing the interests of individuals in their personal information and the interests of organizations in the same.

My recommendations to achieve this goal are three-fold, aimed at improved notification, improved blurring, and limits on how often any single company can obtain geo-immersive imagery. These recommendations parallel my criticisms in Chapter 7, and respectively fall under the following principles of Schedule 1: knowledge and consent, limiting collection, and safeguards. The goal of these recommendations is to strike a balance that allows the continued development of innovative technologies enjoyed by many Canadians, whilst minimizing their potential for widespread social harms.

**Knowledge & Consent**

As discussed earlier, under PIPEDA implied consent can only be relied on by organizations seeking to collect, process, or distribute personal information if the information is of the ‘less sensitive’ variety and if the subjects of that information process have been adequately notified. Yet, I have demonstrated that the existing notification offered by geo-immersive technology providers is woefully inadequate. In the case of Google, to take the paradigmatic example, it is merely a static webpage that is occasionally updated with information regarding broad geographic areas where the Street View cars may be operating. It contains no information at all about how long the image collection will take or which specific areas of a city or town will be imaged on which particular days. It also provides no option for concerned individuals to sign up
for notification of when their neighbourhood might be imaged by the cameras, instead requiring
them to check the website daily to see if there have been in changes or updates. I have also
argued that this inadequate notice makes it challenging for individuals to accurately predict
when they may be subject to geo-immersive surveillance, and consequently their exposure to the
unseen audience. Interpreting privacy in a relational fashion suggests that we ought to, in
contrast, seek to grant the individual the ability to control their exposure to the greatest extent
possible, whilst still balancing off the interests of organizations, as is the mandate of PIPEDA.

I therefore propose clause 4.3.6 of PIPEDA be amended to make it more explicit that notice is
required in the case of implied consent. While the OPC has already interpreted implied consent
in this fashion, making notice a specific requirement would make it easier to defend a more
rigorous standard of applicable notice. Indeed, given that per Austin, supra, consent has
effectively been subsumed into the question of notice by the OPC, this places greater
importance on the quality of that notice – making it an explicit requirement would assist in this.
I recommend however that the OPC issue specific guidelines on the notice requirement in the
context of commercial geo-immersive surveillance, much as it has done for overt video
surveillance in the private sector.763 The guidelines should indicate that rather than the general
information that is provided now, service providers ought to provide detailed information about
the expected locations of camera-equipped cars along with more precise information about the
timeframe when they are expected to be operating. This would not need to be on a real-time
basis (though given the GPS in every car it would certainly be feasible), because creating a real-

763 See “Guidelines for Overt Video Surveillance in the Private Sector”, Office of the Privacy Commissioner of
20, 2013.
time map of all currently active camera-equipped cars would likely create safety hazards, given
the interest some individuals have shown in participating creatively in geo-immersive imagery.
Accuracy of a particular city over a particular number of days, along with expected hours of
operation would likely be sufficient.

Second, enhanced notification requirements would require any service provider wishing to
engage in geo-immersive surveillance to adopt a dynamic notification system that allows
Canadians to sign up for ‘email alerts’ that could be triggered by provision of their postal code.
When a geo-immersive provider has selected an area for initial or updated imagery collection,
anyone whose postal code falls within that area could be automatically notified via email, with
information about proposed dates, length of recording, type of recording (i.e. video or still
photography). While this information would only be available automatically to those who
voluntarily subscribed, it would nonetheless be a great improvement over the existing system.
Indeed, to their credit Google has already adopted a slightly improved notification approach in
several European countries after complaints from their data protection authorities. Following
negotiations, in 2009 Google announced that in those countries they would announce
through the press when imaging would take place.764 While press notifications are not as effective as the
system I have proposed, there is no reason that this intermediary level of protection ought not to
be immediately available to Canadians.

---

online at http://googlepolicyeurope.blogspot.ca/2009/06/street-view-exploring-european-streets.html, last accessed
Sep 3, 2012.
There are limits to the effectiveness of notification, however. It would be technically feasible, for instance, for each ‘Street View’ car (or similar vehicle) to send updates to every active mobile phone in an area that it was entering for the purposes of imaging. While not everyone might carry a mobile phone, the penetration rate of such devices in Canada suggests that a majority would. For the sake of argument, let us presume that such a system was broadly accepted and accessible to a large majority of the population. In such a case, the ‘notification’ requirement would surely be met. But if the vehicles or other devices were roaming constantly, such a system might serve to only remind people of how frequently they were under surveillance, and therefore might spur the very panoptic harms I earlier identified. In some sense then, highly detailed notice might actually be counterproductive to my goals. Thus, it is necessary to combine enhanced notification procedures with more stringent rules on the frequency with which imaging can occur. Notification – no matter how effective – without other protections would serve only to justify surveillance, rather than limit it.

Limiting Collection

I earlier criticized the OPC’s interpretation of PIPEDA’s clause 4.4 in the context of public street surveillance, but I have also accepted that this kind of ‘indiscriminate’ collection of personal information is a necessary consequence of the way geo-immersive technologies operate. A better interpretation of ‘limiting collection’ in the context of commercial public street surveillance is therefore to consider it a limitation on the frequency with which images can be taken, and on the kinds of images that can be taken. Again, this could be accomplished through the issuance of guidelines by the OPC.
Such guidelines ought to include a limit on the frequency with which any particular geo-immersive technology service provider can ‘re-take’ imagery of an area they have already photographed. Certainly, service providers have an interest in having up-to-date and accurate images as part of their system. But as I have argued, there is the potential for it to either become much more intense in the future as corporations compete with one another to have the most accurate, detailed, or current information. Thus, even though it is true that typically it appears as though geo-immersive service providers do not collect imagery of any particular area more once or twice a year, that may change in the future. I therefore propose that a limit be created for geo-immersive surveillance that allows the collection of imagery no more than once per year in any given place, subject to exceptions for technical errors in the collection, or particular events of public interest (such as the Olympic coverage Google provided in Vancouver).

Guidelines also ought to be issued regarding the form of image collection. Currently, geo-immersive providers are only collecting ‘still’ imagery, but there is nothing in the current OPC interpretations of their practices that would necessarily prevent them from recording video. In the state context, the OPC has noted that video surveillance is more problematic than the recording of still images, suggesting it “at the very least it circumscribes, if it does not eradicate outright, the expectation of privacy and anonymity that we have as we go about our daily business.”765 I would argue that is a legitimate concern in all contexts, including commercial surveillance.

Clause 4.4.3 notes that the limiting collection principle is “linked closely to the… Consent Principle”. One interpretation of this may be that the gathering of video imagery drawn from public places might require stricter consent elements, either in the form of explicit consent from those in the area or physical signs at the boundaries of the area identifying the existence of the surveillance, as the OPC has said is necessary in the context of video surveillance cameras in retail establishments. However, I would argue that an important distinction can be drawn – individuals may have a legitimate choice of whether enter a retail establishment, and even if they do so, video footage is rarely released to the public. In contrast, video surveillance of public spaces would not offer individuals the chance to avoid the cameras other than by avoiding huge swaths of urban areas for potentially days at a time. Thus, I recommend that the OPC issue guidance on this clause to clearly indicate that the widespread collection of geo-immersive video is unacceptable.

Safeguards

Finally, I propose that the OPC more strictly interpret clause 4.7 of PIPEDA, which requires that personal information be protected by appropriate security safeguards. Given that ‘appropriate’ must be read in conjunction with the potential risks associated with the impugned information practice, the OPC ought to issue guidelines requiring any distributor of geo-immersive imagery to undertake to improve the reliability and efficacy of the digital blurring system it uses to mask the identity of those captured in any given image. As I earlier indicated, the existing system, while technically impressive, nonetheless is inadequate to the task of truly obscuring the identity of individuals who are recorded in the images. Service providers must commit resources to developing blurring techniques that result in a far lower probability of identification/re-
identification. This requires not merely a greater level of blurring of faces, but rather the obfuscation of all potential identifying characteristics of an individual. As I argued earlier, identification can be made not only through reference to an inadequately blurred familiar face, but also to dress, gait, body size and shape, etc. This is by no means an impossible technical hurdle. In a conference paper presented in 2010, Flores & Belongi demonstrated an algorithm that could successfully eliminate pedestrians entirely from a Street View style image. Their technique involved pattern recognition of the shape of pedestrians, and then filled in those pixels with duplicates of pixels from nearby spaces in the image, with the result that the pedestrian was effectively made ‘invisible’, without destroying the utility of the geo-immersive project. Figure 25 demonstrates the effect.

Figure 25 – Removing Pedestrians from Street View.

---

766 Arturo Flores & Serge Belongi, "Removing Pedestrians from Google Street View" Computer Vision and Pattern Recognition Workshops (CVPRW), 2010 IEEE Computer Society Conference, [unpublished].

767 Ibid.
In the original image, the imagery reveals a woman walking along an urban street. In the processed image, the woman is barely visible as a ‘ghost-like’ outline. By obscuring her clothes, shape, ethnicity, etc., the chances of her identification are significantly reduced. Not eliminated, however, and thus this improved blurring should not be interpreted as an argument in favour of allowing unrestricted geo-immersive surveillance should it become a viable technique on a commercial product. It is well accepted the even anonymized information can often be ‘de-anonymized’, and impressive technical feats should not cloud our judgment about the potential risks of even blurred images. In any event, it is uncertain whether or not this technique could successfully be implemented on a broader scale; Flores & Belongi admit that their technique does not work well in non-urban areas because it cannot draw on the same kind of surrounding information to make a convincing ‘fill’ of the pedestrian location. In a separate project, Nodari et. al proposed to solve this problem by replacing pedestrians with stock images drawn from an approved data set (see Figure 26).

Figure 26 – Summarization of the steps used to automatically anonymize a pedestrian within a generic cityscape image.\textsuperscript{769}

The advantage again is the obliteration of all cues that may be used to identify an individual, rather than simply blurring their face. Naturally, challenges remain in successfully implementing such techniques on a widespread scale, but it is reasonable to assume that corporations with the vast resources and engineering expertise of Google or Microsoft could improve on such academic projects. In the context of PIPEDA, then, this would be an interpretation of the safeguards principle that geo-immersive service providers use not only current ‘industry best practices’ in their attempts to anonymize individuals captured in images, but that they also make reasonable efforts to \textit{improve} those practices.

\textsuperscript{769} Image taken directly from Angelo Nodari, Marco Vanetti & Ignazio Gallo, ”Digital Privacy: Replacing Pedestrians from Google Street View Images” (2012) 21st International Conference on Pattern Recognition 28889.
The safeguards clause should also be interpreted by the OPC as requiring geo-immersive service providers to provide an option for people to request that their entire residence be subject to blurring, as is now the case in Germany. While according to Google only 2.89% of German homeowners have requested images of their homes be blurred, there is no reason that the same option ought not to be provided to Canadians.\textsuperscript{770} There is also the potential for tighter regulation over the retention of unblurred\textsuperscript{771} images captured by geo-immersive service providers, per clause 4.7.5 of PIPEDA, which reads, “care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.”\textsuperscript{772} For example, Google currently retains unblurred images taken as part of its commercial street surveillance programme for a maximum of one year. This was the result of negotiations with the OPC;\textsuperscript{773} other international data protection agencies have sought (though thus far failed to gain agreement to) shorter periods.\textsuperscript{774} Google’s Chief Privacy Counsel has argued that the twelve-month period is necessary:

\begin{quote}
We think one year strikes a reasonable balance between protecting people's privacy and our ability to reduce mistakes in blurring, as well as use the data we have collected to build better maps products.\textsuperscript{775}
\end{quote}

\begin{itemize}
\item \textsuperscript{770} See “How many German households have opted out of Street View?”, Oct 21, 2010, Google, available online, \url{http://googlepolicyeurope.blogspot.ca/2010/10/how-many-german-households-have-opted.html}, last accessed Sep 12, 2012.
\item \textsuperscript{771} The ‘blurring’ of an image occurs on a duplicate image; it does not irrevocably alter the original image itself.
\item \textsuperscript{772} PIPEDA, Schedule 1, 4.7.5.
\item \textsuperscript{773} See for instance “Letter to Google Inc. regarding the company's proposed retention plan for images collected for its StreetView application”, available online \url{http://www.priv.gc.ca/media/nr-c/2009/let_090821_e.asp}, last accessed Sept 3, 2012.
\end{itemize}
I am content with adoption of the twelve-month period as an industry standard. There have been no (to my knowledge) security breaches of any geo-immersive technology provider regarding their archive of unblurred imagery, and such imagery is never made available to the public (except where the automated system has failed). Since I have encouraged the adoption of more effective blurring techniques, it is necessary to that service providers have the opportunity to refine their abilities on unblurred imagery. Given that at the moment image collection is comparatively infrequent over any one area, and given further that the information collected is likely to be predominantly non-sensitive, it makes sense to allow service providers a period in which they can develop their techniques before being forced to destroy the information. Of course, should these factors change (i.e. a security breach of the unblurred archive), then this interpretation of what should constitute ‘appropriate safeguards’ would likewise change.

A potential counter-argument to these proposed requirements is that they might unjustifiably impact upon the freedom of expression rights of the commercial geo-immersive service providers; the Supreme Court of Canada has held that corporate entities may rely on the expression rights contained in s. 2(b) of the Charter. It might be argued, then, that requiring service providers to blur their images or delete images of pedestrians entirely is an interference with their expressive rights. There potentially two problems with this claim. First, the Charter guarantee only applies expressive activity that “conveys or attempts to convey” a meaning. Given that the service providers have attempted to blur the imagery voluntarily in the past and do not appear to operate the vehicles in a manner that attempts to generate imagery featuring as

---

777 Ibid at p. 969.
many persons as possible, it might be argued that the inclusion of identifiable people within the geo-immersive imagery is not an attempt to convey meaning, and thus does not fall within the ambit of s. 2(b) of the Charter. The second problem is that even if the inclusion of individuals in the images were deemed by a court to be ‘expressive activity’, the restriction may be justified under s. 1 of the Charter through application of the Oakes test. While detailed analysis of this point is beyond the scope of this dissertation, it seems logical to assume that ‘privacy’ would be considered by a court to be a pressing and substantial objective, that requiring effective blurring is a rational response to protecting the identity of individuals, that the service provider’s expressive rights are minimally impaired when they are required to blur, and there is proportionality between that impairment and the goal of protecting the privacy of Canadians. I am therefore content to assume that requiring enhanced technical safeguards in the context of geo-immersive surveillance would pass constitutional scrutiny, even if it is interpreted as a limit on the expression rights of the service providers.

Summary

A stricter interpretation of the Schedule 1 requirements will serve to ensure that geo-immersive technologies remain a viable tool for Canadians whilst limiting their potential for widespread social harm. I have suggested that improved notification procedures would allow for greater certainty as to when someone may be subject to public street surveillance, providing them with a more accurate calculus of their potential for exposure. I also argued that placing strict limits on the frequency of image collection and the types of imagery that can be collected reinforces the idea that while geo-immersive technologies are useful, we do not wish the cost to be a slide into

778 Oakes, supra note 690.
a surveillance society where we are being watched all the time. Finally, I suggested that improved blurring techniques and maintaining limited retention periods would together decrease the risk that anyone who was in fact subject to surveillance could be identified and therefore subject to possible shaming campaigns online. In turn, this would greatly reduce the need for individuals to conform their behaviour to what they perceived were the desired norms of the anonymous watchers. Together, these proposals for a more robust application of the fair information principles found in Schedule 1 of PIPEDA remain consistent with its goal of balancing off the privacy interests of Canadians with the interests of commercial organizations in access to personal information under defined conditions.

These proposals an be justified through reference to the ideas of relational privacy that I earlier outlined – they seek to prevent not only a narrow individual harm when one person loses control over their personal information, but rather are geared towards creating a regime that more severely limits the potential for repeated, low-grade privacy losses occasioned by public street surveillance or other similar technologies. The result is that the ability of individuals to accurately control their exposure is protected, whilst still allowing for organizations to draw information gathered from personal space. Importantly, these proposals are all made under the existing provisions of Schedule 1, with a minor exception that calls for textual recognition of the necessity of notice when an organization is seeking to rely on implied consent. They are, therefore, still consistent with the fair information principles as generally understood.
I contend that these proposals would serve to effectively prevent the widespread harms I have suggested might be associated with geo-immersive technologies from arising by effectively creating a regulatory regime that significantly limits the type of and frequency with which information can be collected by geo-immersive providers, ensures adequate notice is given when such collection does occur, and requires service providers to invest in improved techniques to protect the anonymity of individuals where possible. These proposals serve to control the potential problems I have suggested may accompany a widespread deployment of geo-immersive technologies ‘at source’. Thanks to the bifurcated surveillance infrastructure that characterizes geo-immersive technologies, this will be sufficient to greatly limit the amount of imagery that is available to the end viewers. Rather than attempting to target instances of harassment by those end viewers, which I have suggested is likely to be a difficult process, an effective regulatory regime can be crafted that preserves innovative technologies for use by Canadians whilst limiting their potential to bring broad social harms.

Most interestingly, this also implies that the fair information principles are in fact a sufficient antidote to the kind of surveillance associated with the commercial photography of public space for the purpose of generating maps. This appears contrary to the prevailing wisdom in the surveillance literature, which as I have noted conventionally argues that privacy generally and the fair information principles specifically are insufficient to adequately remedy the harms associated with surveillance. That said, there do remain limits to the usefulness of the fair information principles in other forms of surveillance, however. For instance, PIPEDA would not have any relevance in the context of truly peer-to-peer surveillance, where there was no
commercial organization responsible for the initial collection and publication of the imagery. Should a person surreptitiously take a photograph of someone else in public space and share it with friends, PIPEDA would not apply. This is true despite the fact that such imagery might nonetheless ‘go viral’ through online social networks, and result in individuals being subject to social sanctions in the fashion I have described. New technologies such as the aforementioned Google Glass\textsuperscript{779} might result in the creation of entirely decentralized infrastructure of non-commercial, peer-to-peer surveillance. Such a situation would call for a different kind of regulation than that proposed in this thesis, as PIPEDA and the fair information principles do not apply to non-commercial information practices. I have limited my discussion to a particular form of modern surveillance – commercially-driven digital photography of public space for the purpose of generating explorable maps.

\textsuperscript{779} Supra note 184.
Chapter 9: Conclusion

Geo-immersive Surveillance, Privacy, Autonomy, and the Law

This thesis has considered the implications of a new set of public street surveillance tools known as ‘geo-immersive technologies’ in the areas of autonomy, privacy, and the law. In their current guise, those technologies are commercially developed efforts to digitally map public spaces so that they may be explored by anyone with access to an Internet connection and a sufficiently modern computer. I suggested that while it appears as those service providers currently do not image any one area approximately more than once a year, as the price of the technology drops and competition in the marketplace increases, more companies are likely to compete, and their offerings are likely to be differentiated on the basis of how up-to-date the imagery is and how detailed it is. While necessarily speculative, it is reasonable to expect that while the chance of any one individual being captured in a geo-immersive image is relatively low, this is not likely to be the case in the future.

I therefore sought to consider the effects that more widespread use of geo-immersive technologies might have, and I suggested that it in effect could be seen as forming a system of ‘geo-immersive surveillance’. I noted, however, that the infrastructure of this surveillance is bifurcated in an important fashion – the imagery is collected and initially distributed by a commercial service provider that has no apparent interest whatsoever in the behaviour of those who are captured in it, but there is also a secondary element composed of anonymous end viewers of the imagery. I argued that it is the secondary infrastructure that has the potential to effect behavioural changes on those captured by geo-immersive surveillance programmes. I
showed that already there have been campaigns led by anonymous groups to socially shame or otherwise sanction individuals captured in a digital image violating some kind of social norm. I argued that when this process occurs primarily in an anonymous, online environment, the disinhibition effect associated with such anonymity tends to mean that the sanctions are often disproportionate to the severity of the alleged infraction.

I suggested then that fear of these disproportionate sanctions might lead individuals to modify their behaviour in public as means of avoiding them, and I argued that this was likely to impact minority groups more than others, since (at the moment at least) the members of the digital communities that tend to engage in shaming campaigns are predominantly young, white, and male. I also suggested that minority communities and women who happen to be imaged may be subject to intense scrutiny simply by virtue of their status as “others”, whether or not the image revealed a violation of a particular behavioural norm. I went on to argue that at a certain point, this might lead to the internalization of certain social norms – while people may consciously change their behaviour at first to conform with those norms in public, there is the potential that the conformity will become eventually become automatic. Those subject to scrutiny merely because of their gender, race, or socioeconomic status will not necessarily alter their behaviour to avoid sanction, but will internalize their status as ‘objects’. I connected this to the idea of the Panopticon, which suggests that when subjects cannot be sure when they are under surveillance or when they are not, then they act as though they are always under surveillance. I argued that widespread geo-immersive surveillance not subject to regulation may very well bring about such Panoptic-style effects. When that occurs, not only would public behaviour be modified, but
private behaviour too, and this would bring negative consequences not only for minority communities, but also for a pluralistic and democratic society as a whole, which is strengthened by vibrant debate and discourse. I therefore concluded that widespread geo-immersive surveillance ought to be interpreted as a potential threat to autonomy.

In considering legal tools that might aid in avoiding the aforementioned risks, I argued that despite the criticisms of scholars who have claimed that ‘privacy’ cannot be an antidote to surveillance-related harms, privacy law might in fact serve to effectively regulate the deployment of geo-immersive technologies so that the potential for those harms is greatly minimized. I suggested that the criticisms of privacy in that vein were particularly about an approach to privacy grounded in an individualistic conception of autonomy – one dependant on boundary metaphors about shielding the individual from the collective. Translated into legal tools, this approach to privacy tends to result in spatial questions dominating the analysis, making privacy claims in tort extremely difficult to make out in public space. I also noted that there are many scholars who have rejected such an approach, and argued instead that it is possible to approach privacy from a different perspective and base it on a ‘relational’ account of autonomy, drawn from feminist legal theory.

Instead of being premised upon protecting the individual from obvious ‘invasions’ of privacy and ensuring they retain the ability to withdraw, a relational approach to privacy instead seeks to limit privacy losses that harm the social context within which autonomy can flourish. I suggested that grounding privacy in relational autonomy meshes well with those theorists who
have proposed dialectical accounts of privacy, in which the individual making a privacy claim is engaged in an on-going process of negotiation between the self and the other. On that account, privacy is in large part about controlling one’s exposure, rather than simply the ability to withdraw. I suggested that this can best ground privacy claims in public space, as it lets us understand that we may have legitimate privacy claims as against an unseen, far removed, anonymous audience, despite having sacrificed those claims as against those immediately around us. Relational privacy, I argued, is not best understood as a ‘shield’ or a ‘bubble’ that can be breached or popped, but rather as a blanket that can surround not only ourselves but those around us, and can be both worn down and repaired over time.

I went on to consider two alternative means of legally regulating the spread of geo-immersive technologies. I first considered the likely effectiveness of those captured in an image bringing a civil invasion of privacy claim against the service provider that photographed them without consent in a public space. I demonstrated that under both the statutory torts for invasion of privacy (in the provinces that have them) and under the new common law tort for invasion of privacy that has emerged in Ontario, it would appear impossible for an individual to mount a successful action against a geo-immersive technology service provider. This impossibility stems from a judicial interpretation of privacy that is based significantly upon the public/private dichotomy associated with boundary approaches, with the result that individuals are deemed to have sacrificed their ‘reasonable expectation of privacy’ by virtue of entering public space. Despite the long-standing scholarly criticisms of such approaches, it is clear that those critiques have not gained traction with the Canadian judiciary in their deliberations about invasion of
privacy torts. I also suggested that even if a tort could be created that was more responsive to a relational account, it is unlikely that private law actions would be a useful tool in any event, due to the risk that they would invariably catch innocuous ‘watching’ behaviour or photography in public places. I concluded that actions in tort simply are not the correct tools for addressing low-grade but systemic surveillance.

I therefore went on to consider Canada’s data protection legislation, PIPEDA, with the idea that it was not necessarily reflective of a spatial orientation to privacy. I noted that while a ‘control’ approach to privacy, as PIPEDA reflects, has also been criticized as being designed to respond to isolated invasions of informational privacy, the effects of such a regime might be much broader. I suggested that while PIPEDA is indeed based around the idea of granting control to the individual over his or her personal information, the bifurcation of the infrastructure between the ‘collectors’ and the ‘viewers’ that characterizes geo-immersive surveillance opens up the possibility through regulation via the fair information principles. This means that, properly implemented, PIPEDA contains the means by which the growth of geo-immersive surveillance infrastructures can be significantly controlled. This suggests that data protection laws may in fact be responsive to certain surveillance-related harms, despite the apparent handicap of being based upon an individual’s right to control their personal information. I went on to suggest that the principles of relational privacy could be used to justify a more robust implementation of the fair information principles in the context of geo-immersive surveillance. I considered ways in which three of the requirements under Schedule 1 of PIPEDA could be implemented in a way that was more responsive to low-grade surveillance harms, whilst still remaining consistent with
the text of PIPEDA. I suggested that improving the notice requirements that appear necessary before ‘implied consent’ can be relied upon under the ‘knowledge and consent’ provisions, limiting the frequency with which images can be taken and the type of recording that can be allowed in public space under the ‘limiting collection’ provisions, and strengthening the kinds of anonymization techniques used on the imagery under the ‘safeguards’ provisions would all be ways of greatly restricting the potential for widespread social harms to arise thanks to the use of geo-immersive technologies. I noted however that all of these changes must be applied – focusing only on notice, for instance, would not serve to limit the growth of geo-immersive technologies in a manner sufficient to significantly lower the probability of surveillance-related social harms from occurring. The lesson is that for the fair information principles to have meaning in regulating surveillance, they must be applied collectively. Importantly, I also noted that none of these changes would prevent Canadians from benefitting from the continued use of innovative technologies that grow out of the digital mapping industry. My recommended approach remains consistent with the purpose of PIPEDA, which is to adequately balance off the privacy interests Canadians have in their personal information with the commercial interests organizations may have in the same.

In legal terms, the problems associated with approaching privacy from a spatially-focused public/private dichotomy appear to be primarily limited to judicial interpretations of the concept of ‘reasonable expectation of privacy’ in civil actions, but a ‘reasonable expectation’ approach is easy to slip into when confronted with technologies that appear to challenge our conventional ideas of public and private. As a straightforward and simple approach to containing privacy
claims, a ‘reasonable expectation’ standard based primarily on spatial considerations may
indeed provide comfort and basic guidance for policy-makers, regulators, and the judiciary.
However, continued reliance on it would serve only to ignore that modern informational privacy
issues overlap significantly with visual surveillance issues – privacy can no longer be
understood only as a tool simply for preventing the ‘peeping tom’, but rather should be
approached as a tool for assisting individuals to control their exposure to an unseen audience of
unknown size whenever they venture into public space. I have tried to show that more nuanced
conceptions of privacy do still have a role to play in regulating the flow of information
generated when in public space. Though the tools themselves are understood in an individual
fashion in order to assist the subject in negotiating the relationship they have between
themselves and ‘the other’, the purpose behind granting the tool is better understood of having a
much broader social dimension too.

This thesis has suggested, then, that the longstanding claims that privacy (generally) and the fair
information principles (in particular) are inadequate when confronted with modern surveillance
is not necessarily correct, at least in the context of commercially-oriented public street
surveillance that collects personal information for the purpose of generating digital maps. While
it is true that surveillance is not only about the gathering of personal information without
consent, I have shown that the fair information principles can be deployed in a fashion that
severely limits the potential of surveillance to reach the “systemic” level required before it is
likely to have widespread effects. Properly limited, collections of personal information drawn
from public space do not necessarily pose more of a threat to autonomy than does being
photographed in public by a newspaper or by a tourist. In the latter two examples, the potential for individual harm exists, by virtue of mockery or shaming, etc., but neither of those examples can realistically be considered a systemic infrastructure of surveillance, and thus the potential harms are limited only to those actually photographed. Data protection legislation, when applied with an appreciation of the relational aspects of privacy, can in fact serve to prevent a systemic structure of surveillance from emerging out of geo-immersive technologies.

There are assuredly limits to this, however. This thesis has offered only a specific set of remedies for a specific challenge – the rise of geo-immersive technologies. I have done so in part by speculating upon the possible future development of those technologies. But since we are in the realm of speculation, it is also possible that my concern about geo-immersive technologies might be ‘pre-empted’ by the rise of another surveillance mechanism. I touched upon the very recent introduction by Google of ‘Glass’, their eyeglasses equipped with a computer, display screen, and camera. I suggested that it might herald the rise of a true ‘peer-to-peer’ surveillance system. Should ‘Glass’ (or similar devices) become a widespread success, it might render futile any attempts to regulate geo-immersive surveillance. By offering the potential to record the ‘point-of-view’ of any ‘Glass’ user non-stop (subject to battery life, one assumes) and to upload that video to the Internet with a single touch, they could represent a surveillance system beyond the fevered dreams of the most paranoid. Lacking the bifurcation upon which geo-immersive surveillance is based, such a system would not be solved by the remedies I have proposed here – no commercial purpose would mean PIPEDA would not apply, and yet claims in tort would still face all the difficulties I have identified in this thesis. The rise

---

780 Supra note 184.
of such a system, therefore, might call for an entirely new regulatory regime. Such speculation is, of course, beyond the scope of this thesis, which has narrowly focused on the harms associated with a particular set of commercially-driven technologies and the possibility of their legal regulation. The growth in non-state surveillance will surely continue to increase in the coming years and will certainly be fruitful area for research. While the result may be the need to develop laws, regulations, and norms different than those mentioned herein, I believe that the concept of relational privacy will remain a useful platform from which to build.
Appendices

Appendix 1 – The OECD Guidelines

Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except:

• a) with the consent of the data subject; or
• b) by the authority of law.

Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

An individual should have the right:

- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- b) to have communicated to him, data relating to him within a reasonable time;
  at a charge, if any, that is not excessive;
  in a reasonable manner; and
  in a form that is readily intelligible to him;
- c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
- d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.
Appendix 2 – The CSA Model Code Provisions\textsuperscript{782}

Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Limiting Use, Disclosure, and Retention, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.
Bibliography

Legislation

(in order of appearance)

*Personal Information Protection & Electronic Documents Act, SC 2000, c 5*

*Criminal Code, RSC 1985, c C-46*

*The Canadian Charter of Rights & Freedoms, Part 1 of the Constitution Act, 1982, being Schedule B to the Canada Act (UK), 1982, c 11*

*Class Proceedings Act, SO 1992, Chapter 6*

*Privacy Act, RSBC 1996, c 373*

*The Privacy Act, CCSM c P125*

*The Privacy Act, RSS 1978, Chapter P-24*

*The Privacy Act, RSNL 1990, Chapter P-22*

*Civil Code of Quebec, SQ 1991, c 64*

*Quebec Charter of Human Rights and Freedoms, RSQ, chapter C-12*

*Interpretation Act, RSC 1985, c I-21*

*The Privacy Act, RSC 1985, c P-21*

Jurisprudence

(in order of appearance)

*R v Ward, 2012 ONCA 660*

*Hill v Church of Scientology, [1995] 2 SCR 1130*

*Warman v Fournier, 2010 ONSC 2126*
AB v Bragg, 2012 SCC 46

Roe v Wade, 410 US 113


Richardson v Davis Wire Industries, Ltd, [1997] BCJ No 937

Doman Forest Products Ltd. v International Woodworkers, Local 1-357, [1990] BCCAAA No 401

St. Mary’s Hospital and H.E.U. (Re), [1997] BCCAAA No 855

Steels Industrial Products v Teamsters, Local 213 [1991] BCCAAA No 500


Malcolm v Fleming, [2000] BCJ No 2400 (BCSC)

LAM v JELI, [2008] BCJ No 1612 (BCSC)

Malner v Manufacturer’s Life Insurance Co. (c.o.b. Manulife Financial), [2005] BCJ No 2632 (BCSC)

Wasserman v Hall, [2009] BCJ No 1932 (BCSC)


Silber (cob Stacey’s Furniture World) v British Columbia Television Broadcasting System, Ltd., [1985] BCJ No 3012 (BCSC)

Heckert v 5470 Investments Ltd., [2008] BCJ No 1854 (BCSC)

Milton v Savinkoff, [1993] BCJ No 2396 (BCSC)

Mohl v University of British Columbia, [2009] BCJ No 1096 (BCCA)

Watts v Klaemt, [2007] BCJ No 980 (BCSC)


Motherwell v Motherwell, [1976] AJ No 555 (Alta CA)


Saccone v Orr, [1981] OJ No 3132 (Ont Cty Ct)

Hunter v Southam, Inc., [1984] 2 SCR 145

Bingo Enterprises Ltd. v Plaxton, [1986] MJ No 185

Lord v Canada (Attorney General), [2000] BCJ No 1206 (BCSC)

Palad v Pantaleon, [1989] OJ No 985 (Ont Dist Ct)

Roth v Roth, [1991] OJ No 1301 (Ont Ct (Gen Div))

Ontario (Attorney General) v Dieleman, [1994] OJ No 1864 (Ont CJ (Gen Div))

Lipiec v Borsa, [1996] OJ No 3819 (Ont CJ (Gen Div))

Dyne Holdings Ltd. v Royal Insurance Co. of Canada, [1996] PEIJ No 28 (PEISC – App Div)


Warman v Grosvenor, [2008] OJ No 4462 (Ont SCJ)

Euteneier v Lee, [2005] OJ No 3896 (Ont CA)


Somwar v McDonald’s Restaurants of Canada, Ltd., [2006] OJ No 64 (Ont SCJ)

Nitsopoulos v Wong, [2008] OJ No 3498 (Ont SCJ)

Caltagirone v Scozzari-Cloutier, [2007] OJ No 4003 (Ont SCJ – Small Claims Court)

Dietemann v Time, Inc., 449 F 2d 245 (Court of Appeals, 9th Circuit) 1971

Roe v Cheyenne Mt. Conf. Resort Inc., 124 F(3d) 1221 at 1236 (10th Circuit) 1997

Hamberger v Eastman, 106 NH 107 (NH Supreme Court 1964)
Nader v Gen. Motors Corp., 25 NY 2d 560 (NY Court of Appeals 1970)

Gill v Hearst Publishing Co., 40 Cal. 2d 224 (Cali SC 1953)

Puckett v American Broadcasting Companies Inc., 917 F 2d 1305 (US Court of Appeals, Sixth Circuit 1990)

Villanova v Innovative Investigative Solutions, Inc. No. A-0654-10T2 (Superior Court of New Jersey – Appellate Division), unreported, July. 7, 2011


Aubry v Editions Vice-Versa, [1998] 1 SCR 591

Sale v Barr, [2003] AJ No 595 (Alta QB)

Robbins v CBC, [1958] Que SC 152

R v Rocha, [2012] AJ No 163 (Alta Prv Ct)

ABC v Lenah Game Meats Pty Ltd, [2001] HCA 63

Grosse v Purvis, [2003] QDC 151

Giller v Procopets, [2004] VSC 113 (Sup Ct of Victoria)

Kalaba v Commonwealth, [2004] FCAFC 326 (Fed Ct)

Campbell v Mirror Group Newspapers, Ltd, [2004] UKHL 22

Peck v United Kingdom, Application no 44647/98, ECHR (4th Section), 28/04/2003

Douglas v Hello Ltd (No 3), [2006] QB 125


Gershwin Publishing Corp. v Columbia Artists Management, 443 F 2d 1159 (2d Circuit 1971)


Rodgers v Calvert [2004] OJ No 3653 (Ont SCJ)
State Farm Mutual Automobile Insurance v Canada (Privacy Commissioner), [2010] FCJ No 889 (FC)

Canada (Information Commissioner) v Canada (Transport Accident Investigation and Safety Board), [2007] 1 FCR 203

Dagg v Canada (Minister of Finance), [1997] 2 SCR 403

Randall v Nubodys Fitness Centres, 2010 FC 681

Wansink v Telus Communications, Inc., [2007] FCJ No 122 (FCA)

Gordon v Canada (Minister of Health), 2008 FC 258

Eastmond v Canadian Pacific Railway, 2004 FC 852

Englander v Telus, 2004 FCA 387

L'Ecuyer v Aéroports de Montréal, [2003] FCJ No 752 (FCTD)

R v Oakes, [1986] 1 SCR 103

AG Quebec v Irwin Toy, [1989] 1 SCR 927

Office of the Privacy Commissioner of Canada Case Findings

(in order of appearance)

PIPEDA Case Summary #2009-008, “Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc.”.

PIPEDA Case Summary #2006-345, “Private school not covered by PIPEDA”.

PIPEDA Case Summary #2009-018, “Psychologist’s anonymized peer review notes are the personal information of the patient”.

PIPEDA Case Summary #2001-25, “A broadcaster accused of collecting personal information via Web site”.

PIPEDA Case Summary #2005-315, “Web-centered company’s safeguards and handling of access request and privacy complaint questioned”.

PIPEDA Case Summary #2005-319, “ISP’s anti-spam measures questioned”.

PIPEDA Case Summary #2006-349, “Photographing of tenant’s apartments without consent for insurance purposes”.

PIPEDA Case Summary #2001-1, “Video surveillance activities in a public place”.


PIPEDA Case Summary #2011-003, “Personal Information Collected in Company’s Defence of Damage Claim Falls Under PIPEDA”.

PIPEDA Case Summary #2003-149, “Individual denied access to personal information”.

PIPEDA Case Summary #2008-394, “Outsourcing of Canada.com e-mail services to U.S.-based firm raises questions for subscribers”.

PIPEDA Case Summary #2009-013, “Publisher collected and used e-mail addresses for marketing without consent”.


PIPEDA Case Summary #2004-269, “Employer hires private investigator to conduct video surveillance on employee”.

PIPEDA Case Summary #2007-388, “Personal relationship between two employees triggers covert surveillance by employer and raises consent issues”.

PIPEDA Case Summary #2008-392, “Individual objects to being photographed by private investigation firm”.

PIPEDA Case Summary #2009-007, “Mother and daughter were videotaped during covert surveillance of another individual”.

PIPEDA Case Summary #2003-131, “Citizen objects to cable company broadcasting street activities on local channel and Web site”.

PIPEDA Case Summary #2011-003, “Personal information collected in company's defence of damage claim falls under PIPEDA”.

PIPEDA Case Summary #2008-396, “Identification machines and video cameras in bars examined”.

PIPEDA Case Summary #2006-349, “Photographing of tenants’ apartments without consent for insurance purposes”.

PIPEDA Case Summary #2007-376, “Condo security company did not misuse security camera system, but improved personal information safeguards”.

PIPEDA Case Summary #2003-114, “Employee objects to company's use of digital video surveillance cameras”.

PIPEDA Case Summary #2004-279, "Surveillance of employees at work".

PIPEDA Case Summary #2004-264, "Video cameras and swipe cards in the workplace".

PIPEDA Case Summary #2005-290, "Video surveillance cameras at food processing plant".

PIPEDA Case Summary #2009-001, "Bus terminal video surveillance is challenged by company employee”.

PIPEDA Case Summary #2006-351, "Use of personal information collected by Global Positioning System considered".

PIPEDA Case Summary #2009-011, "Transit driver objects to use of technology (MDT and GPS) on company vehicles".


PIPEDA Case Summary #2003-226, “Company’s collection of medical information unnecessary; safeguards are inappropriate”.

PIPEDA Case Summary #2009-003, “Insurer discloses individual’s medical information to third-party consultant based on implied consent”.

PIPEDA Case Summary #2003-203, “Individual raises concern about consent clauses on credit card application form”.

PIPEDA Case Summary #2002-42, “Air Canada allows 1% of Aeroplan members to ‘opt out’ of information sharing practices”.

PIPEDA Case Summary #2002-91, “Marketing firm accused of improper disclosure of survey information”.

PIPEDA Case Summary #2003-192, “Bank does not obtain meaningful consent of customers for disclosure of personal information”.

PIPEDA Case Summary #2001-23, “Employee objects to employer’s use of bank account number on pay statement”.
PIPEDA Case Summary #2007-382, “Former employer discloses drug testing information”.

PIPEDA Case Summary #2001-22, “Company asks for customer’s SIN as a matter of policy”.

PIPEDA Case Summary #2010-006, “Rapid oil change shop unnecessarily scanned customers’ vehicle registration information”.

PIPEDA Case Summary #2008-395, “Commissioner initiates safeguards complaint against CIBC”.

PIPEDA Case Summary #2011-008, “Daycare Centre Modified Webcam Monitoring to Increase Privacy Protection”.

PIPEDA Case Summary #2007-386, “Credit card information printed on paper airline tickets not a proper safeguard; transfer of personal information to travel wholesaler questioned”.

Secondary Sources


Flores, Arturo & Serge Belongi, "Removing Pedestrians from Google Street View" Computer Vision and Pattern Recognition Workshops (CVPRW), 2010 IEEE Computer Society Conference [unpublished].


Fried, Charles, "Privacy" (1967) 77 Yale LJ 475.


Gavison, Ruth, "Privacy and the Limits of Law" (1979) 89 Yale LJ 421.


---, "'Cam Era' -- the Contemporary Urban Panopticon" (2003) 1(3) Surveillance and Society 292.


---, "Identity in Ubiquitous Computing" (2005) 23(2) Social Text 95.


Stalder, Felix, "Privacy is Not the Antidote to Surveillance" (2002) 1(1) Surveillance and Society 120.


