

Schulich School of Law, Dalhousie University

## Schulich Law Scholars

---

LLM Theses

Theses and Dissertations


---

2012

### **Social Networking and the Employment Relationship: Is Your Boss Creeping Up On You?**

Michael Keliher

Follow this and additional works at: [https://digitalcommons.schulichlaw.dal.ca/llm\\_theses](https://digitalcommons.schulichlaw.dal.ca/llm_theses)

 Part of the [Labor and Employment Law Commons](#), [Law and Society Commons](#), and the [Privacy Law Commons](#)

---

Social Networking and the Employment Relationship:  
Is Your Boss Creeping Up On You?

by

Michael Keliher

Submitted in partial fulfilment of the requirements  
for the degree of Master of Laws

at

Dalhousie University  
Halifax, Nova Scotia  
August 2012

© Copyright by Michael Keliher, 2012

DALHOUSIE UNIVERSITY

FACULTY OF LAW

The undersigned hereby certify that they have read and recommend to the Faculty of Graduate Studies for acceptance a thesis entitled “Social Networking and the Employment Relationship: Is Your Boss Creeping Up On You?” by Michael Keliher in partial fulfilment of the requirements for the degree of Master of Laws.

Dated: August 23, 2012

Co-Supervisors:

---

---

Reader:

---

DALHOUSIE UNIVERSITY

DATE: August 23, 2012

AUTHOR: Michael Keliher

TITLE: Social Networking and the Employment Relationship: Is Your Boss  
Creeping Up On You?

DEPARTMENT OR SCHOOL: Faculty of Law

DEGREE: LLM CONVOCATION: October YEAR: 2012

Permission is herewith granted to Dalhousie University to circulate and to have copied for non-commercial purposes, at its discretion, the above title upon the request of individuals or institutions. I understand that my thesis will be electronically available to the public.

The author reserves other publication rights, and neither the thesis nor extensive extracts from it may be printed or otherwise reproduced without the author's written permission.

The author attests that permission has been obtained for the use of any copyrighted material appearing in the thesis (other than the brief excerpts requiring only proper acknowledgement in scholarly writing), and that all such use is clearly acknowledged.

---

Signature of Author

DEDICATION PAGE

For the brightest star in my life – my mother, Stella.

# TABLE OF CONTENTS

LIST OF TABLES .....	ix
ABSTRACT .....	x
ACKNOWLEDGEMENTS .....	xi
CHAPTER 1 Introduction .....	1
CHAPTER 2 Setting The Stage: Employment, Privacy, and Socializing via Technology .....	5
2.1 THE IMPORTANCE OF EMPLOYMENT LAW.....	5
2.2 SOCIALIZING AND PRIVACY .....	11
2.3 SOCIALIZING VIA TECHNOLOGY .....	18
CHAPTER 3 Social Networking Explained .....	23
3.1 SOCIAL NETWORKING .....	23
3.2 FACEBOOK BACKGROUND .....	25
3.3 TECHNICAL USE .....	26
3.3.1 USER PROFILE .....	26
3.3.1.1 INFO .....	27
3.3.1.1 NOTES .....	27
3.3.1.1 PHOTOS.....	28
3.3.1.1 FRIENDS .....	28
3.3.1.1 WALL .....	29
3.3.2 STATUS UPDATE.....	29
3.3.3 TAGGING .....	29
3.3.4 NEWS FEED .....	30
3.3.5 MESSAGES .....	31
3.3.6 COMMENTING .....	31
3.3.7 THE "LIKE" BUTTON .....	32
3.3.8 CHAT .....	32
3.3.9 EVENTS.....	33
3.3.10 GROUPS .....	33
3.3.11 PAGES .....	33

3.3.12 SEARCH BAR .....	34
3.3.13 POKES .....	34
3.3.14 NOTIFICATIONS.....	35
3.3.15 TIMELINE .....	35
3.3.16 SEE FRIENDSHIP .....	36
3.3.17 FACEBOOK MOBILE.....	36
3.4 PERSONAL INFORMATION.....	36
3.5 FACEBOOK PRIVACY.....	37
3.5.1 PUBLIC .....	39
3.5.3 FRIENDS AND NETWORK.....	39
3.5.3 FRIENDS AND FRIENDS OF FRIENDS.....	39
3.5.4 FRIENDS.....	39
3.5.4 CUSTOM .....	40
3.6 ACTIVITY LOG .....	41
3.7 FAKE ACCOUNTS AND LOGIN INFORMATION SHARING.....	41
3.8 USE OF FACEBOOK .....	43
3.9 “CREEPING” .....	43
3.10 PRIVACY COMMISSIONER ISSUES .....	44
CHAPTER 4 The Current Landscape of Canadian Privacy Law.....	47
4.1 <i>PRIVACY ACT</i> .....	49
4.2 <i>PROVINCIAL PUBLIC SECTOR PRIVACY LEGISLATION</i> .....	51
4.3 <i>PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT [PIPEDA]</i> .....	53
4.4 <i>PROVINCIAL PRIVATE SECTOR PRIVACY LEGISLATION</i> .....	56
4.4.1 <i>PERSONAL INFORMATION PROTECTION ACT OF BRITISH COLUMBIA [PIPA BC]</i> .....	57
4.4.2 <i>PERSONAL INFORMATION PROTECTION ACT OF ALBERTA [PIPA AB]</i> ..	61
4.5 <i>TABLE 1</i> .....	64
4.6 THE TORT OF INVASION OF PRIVACY.....	66
4.6.1 <i>TORT CREATED BY STATUTE</i> .....	66
4.6.2 <i>RIGHT TO PRIVACY AT COMMON LAW</i> .....	68

CHAPTER 5	Application to the Pre-Employment Phase .....	74
5.1	APPLICATION OF EMPLOYMENT STANDARDS LEGISLATION.....	78
5.2	DEGREES OF INVASIVENESS .....	80
5.2.1	PASSWORD.....	80
5.2.2	PUBLIC .....	81
5.2.3	IN-BETWEEN.....	81
5.3	A RISK FOR EMPLOYERS: HUMAN RIGHTS .....	82
5.4	ANOTHER RISK FOR EMPLOYERS: UNFAIR LABOUR PRACTICES.....	86
5.4	SPECIFIC LEGISLATION .....	87
5.5	BRITISH COLUMBIA NDP INVESTIGATION .....	90
5.6	FACEBOOK’S REACTION .....	93
5.7	PRIVACY COMMISSIONER SOCIAL NETWORKING BACKGROUND CHECK GUIDELINES .....	94
CHAPTER 6	Application of Current Law to the Employment Phase .	101
6.1	EMPLOYEE MONITORING IN THE WORKPLACE .....	101
6.2	MONITORING OF AT-WORK COMPUTER ACTIVITY.....	104
6.3	EMPLOYER CONCERNS REGARDLESS OF LOCATION .....	108
CHAPTER 7	New Virtualism Explained .....	124
7.1	THE PERMEABILITY OF REAL AND PERSONAL SPACES.....	128
7.2	RECOGNIZING THE IMPORTANCE AND INTERDEPENDENCE OF PERSPECTIVE .....	130
7.3	REJECTING THE LEGAL IMMUNITY THESIS.....	132
7.4	PRIVACY IN NEW VIRTUALISM .....	133
7.5	INFORMATIONAL PRIVACY: A PROBLEM .....	134
7.6	PERSONHOOD IN CYBERSPACE .....	136
7.7	THE CONCEPTUAL ADVANTAGE .....	139
CHAPTER 8	Application of New Virtualism .....	146
8.1	PRE-EMPLOYMENT .....	146
8.2	DURING WORKING HOURS .....	156
8.3	GENERAL SOCIAL NETWORKING ACTIVITY .....	158
CHAPTER 9	Conclusion.....	168
	BIBLIOGRAPHY.....	172



LEGISLATION .....	172
JURISPRUDENCE .....	174
SECONDARY MATERIALS.....	176
OTHER SOURCES.....	180

## LIST OF TABLES

<b>Table 1</b> ....Summary of relevant provisions of privacy legislation.....	64
---	----

## **ABSTRACT**

There are currently over 900 million Facebook users worldwide (and counting). With increased use of social networking comes new concerns for personal privacy and control of social networking information. More and more, Facebook activity trickles its way into offline contexts, perhaps none more so than the employment context. A new trend in the hiring process is social networking background checks, where some employers go so far as to request a candidate's Facebook password. Not only this, but the frequency of Facebook activity resulting in employment law disputes is increasing, and has even been found to constitute sufficient grounds for discipline and termination. This thesis examines the current privacy protection given to social networking information in the context of the employment relationship, highlights problems with the current legal landscape in this regard, and offers an emerging theory, New Virtualism, as a conceptual basis for the regulation of this issue going forward.

## **ACKNOWLEDGEMENTS**

I wish to express my most sincere appreciation to the Schulich School of Law and the people that make it such a fantastic learning environment. I am especially grateful to my co-supervisors, Dianne Pothier and Bruce Archibald for their guidance throughout this entire process. Without their vast reserve of patience and knowledge, this thesis would have never been completed.

I also thank my loving family, whose constant support serves as the catalyst for all that I am able to accomplish.

## **CHAPTER 1      Introduction**

The use of computers in the workplace has expanded dramatically over the past half-century or so. Once upon a time, computers were used simply as devices for typing. The vast majority of employees would not engage in computer use at all; rather, there would be people employed in administrative assistant positions for the specific purpose of typing. As the technology evolved, the process of typing became more forgiving and because it required less specific expertise, more people began to engage in the typing process. Over time, the functionality and use of computers in the workplace expanded, developing the capacity for data analysis and completion of other tasks that were formerly carried out by employees alone. Then, computers became even more multi-faceted with increased storage capacity, word processors made typing documents easier than ever before, and it became practical and efficient for most employees to engage in computer use to carry out their everyday tasks. Eventually, with the introduction of internet technology, not only are more and more people using computers and the internet on a daily basis at work, but more and more people are using computers and internet technology in their personal lives. However, not only does this increased use of computers and internet technology present a convenient and efficient way to complete tasks at work and in one's personal life, but the resulting degree of pervasiveness presented by such computer use increases correspondingly – the recording of an ever increasing amount of

personal information on both personal and work computers has become the norm, rather than the exception.

A relatively new way in which a growing number of individuals are using computers and internet technology is as a medium to socialize with one another. While it is possible for people to socialize in any number of ways via computers and internet technology (e.g. email, message boards, etc.), social networking sites, specifically Facebook, have dramatically changed the manner and extent to which many people interact with one another online. As a result of the electronic, online nature of this form of social interaction, there exists on Facebook's server a permanent record of the social activity of members of these virtual communities. If someone were to gain access to this information, he or she has the potential to have access to some of the most intimate details of a person's life – his or her likes and dislikes, who he or she interacts with, what they speak about, and the list goes on. Nonetheless, despite this apparent risk, the number of people who choose to participate in social networking sites grows every day. As a result, so to do the associated risks that come with participation in social networking. Consequently, the legal protection that is afforded to our social networking information is vital – if the information collected about us on computers is not adequately protected, personal privacy can be essentially obliterated.

Given the abundance of information that can be found out about an individual by examining his or her social networking activity, there is an

emerging practice where employers perform what is known as a ‘social media background checks,’ on job candidates – what these background checks amount to is simply “creeping”<sup>1</sup> a candidate’s social networking profile. Not only this, but during the employment relationship, employers are monitoring the social networking activities of employees, and more and more often social networking activity is becoming the basis of employment law disputes.

The technology associated with these sites and the ability to record the information contained on computers through the use of computer software are progressing at an extremely rapid pace – as a result, personal privacy is in danger. However, given the relative newness of this activity, courts and legal scholars are still struggling with just how to address and conceptualize an individual’s privacy interests and rights in his or her social networking activity in the employment context. The purpose of this work is to assess how we are doing in this regard – whether we are getting it right. Or, more accurately, the purpose of this work is to explain how we are getting it wrong.

In Chapter 2, I will set the stage as to why this issue is important – I will outline the role of employment law, examine the importance of socializing and privacy, and explore the notion of socializing via technology. For those readers who are unfamiliar with social networking, Chapter 3 will explain its “ins and outs” with a particular emphasis on the most popular social networking site, Facebook. Chapter 4 will provide an overview of the

---

<sup>1</sup> The meaning of “creeping” will be explained in Chapter 3.

current landscape of privacy law in Canada. In Chapters 5 and 6, I will apply Canadian privacy law to the pre-employment and employment phases, respectively. In Chapter 7, I will explain “New Virtualism,” an emerging area of scholarship that I contend presents a theoretical basis and framework for the way we should conceptualize the protection of social networking information in the employment context. In Chapter 8, I will apply New Virtualist principles to the problems presented in Chapters 5 and 6. And finally, in the Conclusion, I will summarize my findings and propose a general direction for improvements going forward.



## **CHAPTER 2      Setting The Stage: Employment, Privacy, and Socializing via Technology**

### **2.1    THE IMPORTANCE OF EMPLOYMENT LAW**

Something that is important for a healthy society is to create an environment where people are able to work under good, humane, circumstances. In contemporary Canadian society, it is not uncommon when meeting someone new to ask, “What do you do?,” or more specifically, “What do you do for a living?” This is a perfectly normal, and acceptable question to ask someone. What is sought by these questions is to find out the kind of work to which the person devotes much of his or her time, or what kind of job he or she works for subsistence. The reason for asking could be curiosity, or simply making conversation; either way, the goal of such a question is to find out more about what the person does with his or her time. Work, first and foremost, is a way for us to satisfy our material ‘wants’. At its most basic level, our ‘wants’ are actually our ‘needs,’ in that they are what we need for survival (i.e. food, shelter, clothing, etc.). Once our ‘needs’ are met, the amount and nature of a person’s work is often in some way dictated by the lifestyle he or she wishes to lead, or vice versa.

Income generation has not always been the primary means by which a person obtained their livelihood.<sup>2</sup> As late as the eighteenth century, for most

---

<sup>2</sup> Raymond Edward Pahl, “Editor’s Introduction: Historical Aspects of Work, Employment, Unemployment and the Sexual Division of Labour” in Raymond

people and families, subsistence was dependent upon a mix of task work at the household (for example, farming), as well as some income generating wage labour.<sup>3</sup> It was not until the nineteenth century that “the notion that one should obtain most, if not all, of one’s material wants as a consumer by spending the money gained through employment [first] emerged.”<sup>4</sup> In contemporary Canadian society, there are very few practicable opportunities for someone to earn their livelihood not within the societal institution of the employment relationship.<sup>5</sup> As a result, “the means by which the personal meaning of work is attained are now effectively controlled by others.”<sup>6</sup>

In Canada, where the needs of subsistence can be taken care of by a fraction of the population, leaving the rest to work providing services that are divorced from the imperatives of survival, work becomes more so about personal development and fulfillment than merely about physical survival.<sup>7</sup> As Beatty illustrates in the following passage, work is one of the principal modes of individual expression and identity in our society:

At its most basic level, this personal end of the relationship is one of subsistence, of physical survival. As we have noted, for most individuals in our society, their physical needs can only be satisfied within this institution. However, at a more

---

Edward Pahl, ed., *On Work: Historical, Comparative and Theoretical Approaches* (Oxford: Basil Blackwell, 1988) 7 at 11-12 [*On Work*].

<sup>3</sup> Pahl, *On Work*, *ibid*.

<sup>4</sup> Pahl, *On Work*, *ibid*.

<sup>5</sup> David Beatty, “Labour is Not a Commodity” in Barry Reiter & John Swan, eds., *Studies in Contract Law* (Toronto: Butterworths, 1980) 313 at 318-324 [*Labour is Not a Commodity*].

<sup>6</sup> Beatty, *Labour is Not a Commodity*, *ibid* at 321.

<sup>7</sup> Beatty, *Labour is Not a Commodity*, *supra* at note 5, 318.

sophisticated level, and reflecting the characterization of humans, for the most part, doers and makers, the identity aspect of employment is increasingly seen to serve deep psychological needs as well. It recognizes the importance of providing the members of society with an opportunity to realize some sense of identity and meaning, some sense of worth in the community beyond that which can be taken from the material product of the institution. As a vehicle which admits a person to the status of a contributing, productive, member of society, employment is seen as providing recognition of the individual's being engaged in something worthwhile. It gives the individual a sense of significance.<sup>8</sup>

Contrast this with the following passage from sociologist William Julius

Wilson on the effect of unemployment on people:

In the absence of regular employment, a person lacks not only a place in which to work and the receipt of regular income but also a coherent organization of the present — that is, a system of concrete expectations and goals. Regular employment provides the anchor for the spatial and temporal aspects of daily life. It determines where you are going to be and when you are going to be there. In the absence of regular employment, life, including family life, becomes less coherent. Persistent unemployment and irregular employment hinder rational planning in daily life, a necessary condition of adaptation to an industrial economy.<sup>9</sup>

As can be seen from these two passages, employment is a very important part of an individual's life – the employment relationship is a centrally organizational mechanism in society. Employment not only provides people with a source of income, but it provides people with a sense of identity and purpose, as well as a sense of stability in their lives. Suffice it to say,

---

<sup>8</sup> Beatty, *Labour is Not a Commodity*, *supra* at note 5, 324.

<sup>9</sup> WJ Wilson, "When Work Disappears: New Implications for Race and Urban Poverty in the Global Economy" (1999) *Ethnic and Racial Studies* volume 22 number 3 p 479 at 482.

employment is a major part of an individual's life in contemporary Canadian society.

The nature and dynamics of the employment relationship within a society is not only important to the individuals within that society, but it is also important to the wellbeing of the society as a whole. In an increasingly global economy, it can be said that there is a direct correlation between the productivity of a nation's workforce and its economic prosperity, as well as its social and political environment. Such environmental factors will strongly influence what kinds of demands are placed upon our workforce. This will no-doubt affect the way we, as a society, view the purpose served by basic social institutions like the employment relationship, and in turn, affect the way in which they are regulated by law.<sup>10</sup>

In Canada, jurists and legislatures, "influenced by social evolution and human experience in this country, have created employment laws that reflect their views on what is required to ensure justice in the workplace and the redistribution of losses flowing out of the employment relationship."<sup>11</sup> What is considered in the evolution of employment law are the interests and situation of the employer, the interests and situation of the employee, the societal interests in employment as an institution, and parties external to the employment relationship, but who are nonetheless affected by the existence

---

<sup>10</sup> Beatty, *Labour is Not a Commodity*, *supra* at note 5, 318.

<sup>11</sup> Labour Law Casebook Group, *Labour and Employment Law: Cases, Materials, and Commentary*, (Toronto Irwin Law: 2004) 7<sup>th</sup> ed at 1-2 [*Labour and Employment Law: Cases, Materials, and Commentary*]

of the employment relationship. Canadian labour and employment law is conventionally seen as consisting of three closely interrelated regimes.<sup>12</sup>

The first regime is the common law of employment, which basically treats the contract between the employee and the employer for the buying and selling of labour as the cornerstone of the employment relationship.<sup>13</sup> The principles of contract law alone, however, have proven insufficient in securing workplace justice.<sup>14</sup> This is because there is an assumption in contract law that a contract is the result of relatively free bargaining between parties with relatively equal bargaining power.<sup>15</sup> “For most workers, however, this assumption is not true; their employer has the power to dictate the terms of employment on a take it or leave it basis.”<sup>16</sup> It is almost universally accepted by labour and employment lawyers and lawmakers that the employee suffers an inequality of bargaining power *vis-à-vis* an employer and an important purpose of labour and employment law is to balance out this inequality.

The second regime is the substantive approach to balancing out the inequality in bargaining power – which essentially means a statutory re-

---

<sup>12</sup> *Labour and Employment Law: Cases, Materials, and Commentary*, *ibid* at 1-1.

<sup>13</sup> *Labour and Employment Law: Cases, Materials, and Commentary*, *ibid* at 95.

<sup>14</sup> *Labour and Employment Law: Cases, Materials, and Commentary*, *ibid* at 95.

<sup>15</sup> *Labour and Employment Law: Cases, Materials, and Commentary*, *ibid* at 95.

<sup>16</sup> *Labour and Employment Law: Cases, Materials, and Commentary*, *ibid* at 95.

writing of the resulting employment contract. These substantive interferences amount to enacting standards that will work to govern the employer-employee relationship.<sup>17</sup> These include statutes such as human rights legislation, employment standards legislation, occupational health and safety legislation, etc. They regulate such matters as hours of work, minimum wage, maternity leave, workplace standards, etc. The idea behind these is that the state is ensuring that a social minimum is attained for workers through a ‘floor’ of basic standards.<sup>18</sup>

The third regime is to approach the balancing act that places emphasis on the collective power of employees – an area of law that is usually referred to as ‘labour law’ as opposed to ‘employment law.’ This is a way of turning up the bargaining power valve on the employee’s side through procedural means – we substitute the individual with the collective, and allow for collective bargaining with an employer.<sup>19</sup> The idea is that there is strength in numbers, and opening up a procedure for employees to work together to negotiate a collective agreement with an employer is more likely to result in a contract that is the product of less unequal bargaining.

As can be seen by this brief overview of Canadian labour and employment law, an important purpose of said law is to strike a balance

---

<sup>17</sup> *Labour and Employment Law: Cases, Materials, and Commentary*, *ibid* at 750.

<sup>18</sup> Brian Langille, “Labour Law is a Subset of Employment Law” (1981) 31:2 UTLJ 200 at 202.

<sup>19</sup> Brian Langille, “Labour Policy in Canada: New Platform, New Paradigm” (2002) 28 Can Pub Pol’y 133-142. [*New Platform*].

between the interests of all those who are involved in the employment relationship, keeping in mind the inequality in bargaining power that exists between an employer and an employee.

As a final note for this discussion of the legal regulation of the employment relationship, while easily observable by any working person in 21<sup>st</sup> Century Canada, it is important to note that with every passing day, more and more of Canada's workforce is using computers and technology to accomplish its goals. As a result, there have recently been many new employment issues that have arisen as a result of this spike in technological use and work. Such issues will be discussed in greater detail in Chapter 6.

## **2.2 SOCIALIZING AND PRIVACY**

While a person's working life does define a major part of an individual's sense of identity, there is also much more to a person's identity than the job he or she has. A person's job alone does not make up a person's identity, or account completely for an individual's sense of fulfillment. A major part of being a living human on earth is interacting with other living humans – human beings are social animals. The degree to which we interact with others varies, and the level of intimacy in those relationships between humans also varies; however, the likelihood of there being a person living in our society who did not interact with anyone, and did not have any kind of relationship with any other person is extremely unlikely. These interactions

and relationships work to shape the course of an individual's life, either directly or indirectly.

Despite our desire to socialize, we often hear people claim that something is a “violation of their privacy,” or that they “just need some privacy.” This is because something else human beings value is our privacy – but what exactly *is* privacy? The Oxford English Dictionary defines “privacy” as follows: “The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; seclusion; freedom from interference or intrusion.”<sup>20</sup> While this definition is a pretty good one, it does not explain the essence of the importance of privacy, or the extent to which we should have a right to privacy. Furthermore, this definition of privacy, “the state or condition of being alone,” seems to be at odds with the other fundamental human desire to socialize. A person's right to privacy has been given countless different legal interpretations and meanings, varying in scope depending on the context in which a privacy issue arises, and the legislation that may apply to that situation. Under Canada's legal system, the degree to which an individual can reasonably expect privacy varies significantly depending where he or she is, whom he or she is with, and what he or she is doing – context is everything. This emphasis on context shows that privacy is not only about an individual's ability to be left alone.

---

<sup>20</sup> *The Oxford English Dictionary*, 2d ed, *sub verbo* “privacy”, online: Oxford English Dictionary <<http://www.oed.com>>.



In the article, *Virtual Communities and the Social Dimension of Privacy*, Janis Goldie has written that privacy is not only about the individual, but rather, there is a very important social dimension to privacy, where “the other” plays an integral role in how the individual conceptualizes privacy:

[looking at privacy on an individual level], privacy is seen as protecting the autonomy of the individual, the desired intimacy level for each individual, and the individual's right to choose and act in various social roles. However, there is always an implicit reference to "the other" when discussing privacy. Autonomy is inherently about autonomy from others, intimacy is about intimate relations between oneself and others, and the social roles one chooses to enact are for other people. Furthermore, the degree of accessibility to others and the amount of information one wants others to have are all connected to privacy. In this way, privacy is essentially a social concept --at its very core, privacy has to do with our relations with others. Privacy is about facilitating associations with people, not about creating independence from people.<sup>21</sup>

What this implies is that “the other” is key to how individuals determine the degree to which they want privacy. This is to say that privacy is really about having the ability to choose with whom, and to what extent, we let others into our lives.

Furthermore, it is not only the individual, but society as a whole that benefits from the legal recognition of an individual’s right to privacy. In Canada, we have a constitutional right to be secure from unreasonable search

---

<sup>21</sup> Janis L Goldie, “Virtual Communities and the Social Dimension of Privacy” (2006) 3:1 UOLTJ 133 at paragraph 18 [*Virtual Communities and the Social Dimension of Privacy*]

and seizure by state actors.<sup>22</sup> In conceptualizing this right, the Supreme Court of Canada has explicitly acknowledged that “the restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.”<sup>23</sup> If the government does not have any restraints on the degree to which it can pry into the lives of citizens, freedoms essential to the democratic process, like freedom of speech and freedom of association, can be significantly reduced, and perhaps rendered meaningless.<sup>24</sup> Without such freedoms, the extent to which we are able to organically progress in a manner that is reflective of the true wishes of citizens is stifled.

The societal interest in privacy does not only pertain to privacy from an unfettered watch by the state, but also from other private actors. If we feel that other citizens are constantly able to unwelcomely observe us, we will feel that we are constantly subject to the threat of unsolicited judgment, correction, and criticism;<sup>25</sup> we would essentially be reduced to living our lives like children, fearful that any of our actions could be brought back in the future and used against us. Our individuality will be suppressed if everything we do in our personal lives is observed and recorded by

---

<sup>22</sup> See *Canadian Charter of Rights and Freedoms*, R.S.C, 1985 Appendix II, No. 44 s. 8 *see also* Part I (ss. 1 to 34) of the *Constitution Act, 1982*.

<sup>23</sup> *R v Tessling*, 2004 SCC 67, [2004] 3 SCR 432, 244 DLR (4<sup>th</sup>) 541 at paragraph 3 [*Tessling*].

<sup>24</sup> Priscilla Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (Chapel Hill: The University of North Carolina Press, 1995) at 221-230.

<sup>25</sup> I say unsolicited criticism here, because I am not including certain welcomed types of criticism that are acceptable (i.e. work performance reviews).

unwelcome audiences. The result of such a society would be one where creativity is suppressed, uniqueness is not appreciated, and as a result, human progress is stymied.

A common retort to those who advocate for privacy is that, ‘if you are not doing anything wrong, then what do you have to hide?’ The problem with such an idea is that it presumes that privacy is about hiding something wrong. We are not doing something wrong when we go to the bathroom, or when we seek out a secluded place to have an intimate conversation. We are not doing anything wrong when we write a personal journal, or write a letter to a friend. We seek out different degrees of privacy when we do these things, essentially, because they are exclusively **our** business. If we are not able to find a private place to use the bathroom, we may not go until it is absolutely necessary. If we cannot find a private place to have an intimate conversation, we may forgo the conversation completely. And if we know that our personal journal or personal correspondence is free for all others to read, then the content of what we write in that journal or correspondence will be altered significantly, or we may not write such a journal or correspondence at all. The idea is that if we do not have privacy, our demeanor changes regardless of whether we are doing something that is socially acceptable. Our actions are filtered, and our individuality is suppressed. Privacy is about having the ability to reasonably choose our audience, or to reasonably choose to have no audience whatsoever – privacy is important for a healthy society.

In addition to the aforementioned constitutional protection of privacy in the *Charter of Rights and Freedoms*, the common law has evolved to recognize the tort of “intrusion upon seclusion,”<sup>26</sup> and numerous federal and provincial statutes have been enacted with the purpose of protecting the privacy rights of individuals. These legal privacy protections will be examined in further detail in Chapter 4.

The degree of privacy control we have in our social interactions and relationships with other people not only works to shape one’s life externally, they also shape a person’s sense of identity. It is for this reason the real value of privacy is to allow people to choose their audience – not to simply be left alone. Relationships and social interactions serve to play a determinative role in a person’s life that is constitutive of their personhood by virtue of the “*inherently* social nature of human beings.”<sup>27</sup>

Françoise Baylis’s article, *The Self in Situ: A Relational Account of Personal Identity*<sup>28</sup> uses relational theory to unpack how individuals conceptualize their personal identity. Key to relational theory is that individuals are not wholly autonomous beings, but rather,

---

<sup>26</sup> *Jones v Tsige*, 2012 ONCA 32 [*Jones*].

<sup>27</sup> Jocelyn Downie and Jennifer Llewellyn, “Introduction” in Jocelyn Downie and Jennifer Llewellyn, eds, *Being Relational: Reflections on Relational Theory in Health Law* (Vancouver: UNC Press, 2012) at 4 [*Being Relational*] quoting Jennifer Nedelsky, “Reconceiving Autonomy: Sources, Thoughts, and Possibilities” (1989) 7 *Yale JL & Feminism* 7 at 8.

<sup>28</sup> Françoise Baylis, “The Self in Situ: A Relational Account of Personal Identity” in *Being Relational: Reflections on Relational Theory in Health Law* (Vancouver: UNC Press, 2012) at 109 [*The Self in Situ*].

No one is fully independent ... the view of individuals as isolated social units is not only false but impoverished: much of who we are and what we value is rooted in our relationships and affinities with others ... all persons are, to a significant degree, socially constructed ... their identities, values, conceptions, and perceptions are, in large measure, products of their social environment.<sup>29</sup>

According to Baylis, an individual's identity is an amalgam of self-ascription and ascription by others.<sup>30</sup>

It is through our (more or less conscious) interpretations of our values, memories, actions, experiences, and so on as well as the (more or less conscious) interpretations of these same characteristics by others that we come to embody answers to these pivotal questions, thereby instantiating our place in the world as we continually strive for balance between how we see and understand ourselves and how others see and understand us.<sup>31</sup>

When there is a balance between our own conception of ourselves and that which others ascribe to us, there is a state of identity 'Equilibrium;' meaning that the points upon which there is inner and outer congruency are considered to be identity-defining.

We are all complex interdependent beings whose identity is co-constructed and maintained through iterative and cyclical private and public actions, reactions, interactions, and transactions. As we live our lives, constrained in ever-changing ways by our social, cultural, and political environments, as well as by our historical circumstances, we

---

<sup>29</sup> Susan Sherwin, "A Relational Approach to Autonomy in Health Care" in Femenist Health Care Research Network, Susan Sherwin, coordinator, *The Politics of Women's Health: Exploring Agency and Autonomy* (Philadelphia, PA: Temple University Press, 1998) 19 at 34-35.

<sup>30</sup> Baylis, *The Self in Situ*, supra at note 28, 118.

<sup>31</sup> Baylis, *The Self in Situ*, *ibid* at 117.

communicate in overt and covert ways who we are, and we imagine, hope, and despair that others will come to see and understand us as we see and understand ourselves. When this happens (that is, when there is a congruence between self-ascriptions and ascriptions by others), our identity temporarily stabilizes until such time as there is a shift in our identity-constituting self-narrative and we enter a period of disequilibrium, looking once again to restore the balance between how we see and understand ourselves and how others see and understand us. So it is that we are who we say we are and who others will let us be.<sup>32</sup>

It appears that in addition to social activity giving us our own ideas about who we think we are, we socialize with others to get a sense of who others think we are, searching for an ‘equilibrium’ between the way others see us and understand us and how we see and understand ourselves. Privacy, conceptualized as the ability to choose our audience, allows individuals to pursue ‘equilibrium’ in such a way that they can feel a sense of control and security over how they go about defining their own identity. They can feel secure that the parts of their lives that they reasonably wish to stay private can remain private, and the extent and audience for the elements of their life they wish to share with others is also under their control. What privacy allows us to do as individuals is live and contour our lives on this earth together with the relational autonomy necessary for us to achieve a real sense of personhood and identity.

### **2.3 SOCIALIZING VIA TECHNOLOGY**

---

<sup>32</sup> Baylis, *The Self in Situ*, *ibid* at 128.

With the advancement of technology, people are becoming ever more ‘connected’ with one another. I put ‘connected’ in quotations because I do not necessarily mean that people are seeing more of each other’s physical bodies, or interacting more in a physical way, but it is becoming easier and more convenient for people to socialize with one another. This allows more opportunity for individuals to put forth what they believe to be their identity-defining values and features in an effort to achieve identity equilibrium.

Websites that have the effect of making this process easier and more instantaneous are what are known as “Social Networking” sites. I will explore in greater detail the inner-workings of social networking sites, specifically Facebook, in Chapter 3. What these sites allow individuals to do is interact and socialize with one another online. The type of activity that occurs on these sites is more nuanced than e-mail, in that there are many differing levels of interaction, as well as a wide variety of multi-media that can be shared with other people. Part of what makes these sites popular is not just the ease with which they allow people to keep in touch with one another, but sites like Facebook offer a favourable avenue for people to more easily express what they believe to be their “true self,” that may not be so easily expressed in face-to-face-communications.<sup>33</sup> This allows for individuals to put out a narrative of what they believe to be the characteristics that truly

---

<sup>33</sup> Liman Pinar Tosun, “Motives for Facebook Use and Expressing “True Self” on the Internet” (2012) 28 *Computer in Human Behavior* 1510 at 1511 [*True Self*].

define them; the nature of the site makes what the individual puts out observable by others, thus creating a medium through which equilibrium can be assessed and achieved, and, in turn, true, relational identity can be formed. Furthermore, the nature of the way in which people use these sites (navigating in the cyber world as opposed to face-to-face interactions) allows for people to escape the shackles of shyness on a physical level that may, in the physical world, hinder people from showing their true 'self' that they wish for their intended audience to see.

The trickiness with the use of electronic technology and social networking for socializing is that this new way in which we interact causes there to be a record of all of our personal interactions that occur on these sites. Without adequate legal protection and regulation, the existence of such a record can have serious implications for the erosion of personal privacy. More and more, online Facebook activity is trickling its way into offline contexts, perhaps none more so than the employment context. There is an emerging practice of employers performing what are known as 'social media background checks,' on potential employees, and even going so far as to ask for a candidate's social networking login information (meaning not just their login name, but their personal password);<sup>34</sup> not only this, but Facebook

---

<sup>34</sup> Erin Egan, *Protecting Your Passwords and Your Privacy* (23 March 2012) online: Facebook <[https://www.facebook.com/note.php?note\\_id=326598317390057](https://www.facebook.com/note.php?note_id=326598317390057)> [*Facebook Privacy Statement*].



activity and postings have been found to be sufficient grounds for discipline and termination of the employment relationship.<sup>35</sup> This is major!

As mentioned above, there exists legislation and case law that protect personal privacy, and employment standards legislation that protect the interests of employers and employees, but these laws are slow to evolve, whereas technology is evolving at a very rapid pace. While the law can do little to stop the progression of technology, the law can do much to protect the important and valuable aspects of personal interaction with technology. If Facebook and other social networking sites are going to have any real, substantial value in today's world, people need to be comfortable using the sites, and trusting of their inner workings. What is needed are laws that take into account the complicated dynamics of the employment relationship and serve to protect privacy in light of the rapid technological changes and they way these changes are affecting societal norms and the new technological mediums people are using to socialize with one another. Protection of privacy in this context needs to be re-conceptualized and ramped up; if it is not, and the law allows employers to pry into the personal online affairs of employees, work concerns will hang over the employees' heads and the potential that virtual space presents for personal fulfillment through online social activity is compromised.

---

<sup>35</sup> See *Canada Post Corp v Canadian Union of Postal Workers*, [2012] CLAD No 85 (Ponak) [*Canada Post Grievance*].

An emerging approach to the re-conceptualization of how the law should approach online privacy is what is called “New Virtualism.” New Virtualism will be explained in greater detail in Chapter 7. The key aspects of New Virtualism are a perspective that recognizes and acknowledges the distinct nature of virtual space and how people live and interact within that space, and the rejection of the categorization of privacy protection of an individual’s online activity as “informational privacy” in favour of an approach to privacy protection that is more firmly and appropriately based on “informational personhood” in cyberspace.

## CHAPTER 3 Social Networking Explained

Before getting into the details of specific legislation and case law that pertains to social networking and employment law, I will first explain what exactly social networking sites are, and drawing on the most popular social networking site, Facebook, the nature of their use.

### 3.1 SOCIAL NETWORKING

Social Media services are online applications that serve as forums and gathering places in which people can interact, socialize, and share user-generated content with one another. Social Media has been defined as “a group of internet-based applications that build on the ideological and technological foundations of web 2.0<sup>36</sup> and that allow the creation and exchange of user-generated content.”<sup>37</sup> There are six different types of social media: [1] collaborative projects (Wikipedia); [2] blogs and microblogs, (blogspot, Twitter)<sup>38</sup>; [3] content communities (YouTube); [4] social networking sites (Facebook, LinkedIn); [5] virtual game worlds (World of

---

<sup>36</sup> Web 2.0 refers to web-applications that allow for interaction, collaboration, and information sharing online.

<sup>37</sup> Andreas Kaplan, Michael Haenlein, “Users of the World, Unite! The Challenges and Opportunities of Social Media”, (2010) *Business Horizons* 53(1) at 59 [*Users of the World, Unite!*].

<sup>38</sup> While Twitter is listed here as a microblogging site, depending on the way an individual uses his or her Twitter account, it could also be crosslisted as a social networking site. For example, while Twitter can be a microblog, where people blog their thoughts on issues or provide hyperlinks in 140 character-or-less “tweets,” some people also use twitter exclusively as a forum for social interaction among users.

Warcraft); [6] virtual social worlds (Second Life).<sup>39</sup> This work will focus on social networking sites. I have chosen social networking because of the inherently personal nature of a social networking account, as well as employer practices with respect to social networking monitoring, which will be discussed in greater detail in Chapters 5 and 6.

Social networks are websites or web-based services that “allow users to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of others with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.”<sup>40</sup> Facebook is a social networking site owned by Facebook, Inc. that launched in 2004. In 2009, Facebook became the most widely-used social networking site in the world.<sup>41</sup> As of April, 2012, Facebook had over 900 million monthly users, and 526 million users who login to Facebook on a daily basis.<sup>42</sup> Facebook’s mission statement is “to give people the power to share

---

<sup>39</sup> Kaplan, *Users of the World, Unite!*, *supra* at note 37.

<sup>40</sup> Danah Boyd and Nicole Ellison, Social Network Sites: Definition, History, and Scholarship, (2008) *Journal of Computer-Mediated Communication* 13, 210-230 at 211 [*Social Network Sites: Definition, History, and Scholarship*].

<sup>41</sup> Andy Kazeniak, “Social Networks: Facebook Takes Over Top Spot, Twitter Climbs” *CompetePulse* (9 February 2009) online: <<http://blog.compete.com/2009/02/09/facebook-myspace-twitter-social-network/>>

<sup>42</sup> Nicholas Carlson, “Facebook Now Has 901 Million Monthly Users, With 526 Million Coming Back Every Day” *San Francisco Chronicle* (2 May 2012) online: <<http://www.sfgate.com/cgi-bin/article.cgi?f=/g/a/2012/04/23/businessinsiderfacebook-now-has-900.DTL>>

and make the world more open and connected.”<sup>43</sup> On Facebook’s homepage, it is written that Facebook is “free and always will be.”<sup>44</sup> Because it is the most used and elaborate of all social network sites, Facebook will be the social network of choice for explanation and application in this work.

### **3.2 FACEBOOK BACKGROUND**

In 2004, Mark Zuckerberg, who was at the time a Harvard undergraduate student, launched Facebook. Each freshman at Harvard was given a hard-copy photo album of all incoming students; Zuckerberg’s site, then called thefacebook.com, was an online version of this book designed to be used by all students at Harvard.<sup>45</sup> Soon afterwards, the site spread to other universities - Columbia and Stanford.<sup>46</sup> Facebook was much like other social media sites that existed at the time; however, its distinctive feature was its exclusivity, in that it was only available to people who had email addresses at certain universities, and as a result those users could participate in school specific networks.<sup>47</sup> In 2005, Facebook was opened up to high school students, and in 2006, to anyone with an email address.<sup>48</sup>

---

<sup>43</sup> Facebook “Mission Statement” online:  
<<http://www.facebook.com/facebook/info>>

<sup>44</sup> Facebook “Main Page”online: <<http://www.facebook.com/>>

<sup>45</sup> Ilana Gershon, “Un-Friend My Heart: Facebook, Promiscuity, and Heartbreak in a Neoliberal Age” (2011) 84 *Anthropological Quarterly* 865 at 871 [*Un-Friend My Heart*].

<sup>46</sup> Gershon, *Un-Friend My Heart* ibid.

<sup>47</sup> Gershon, *Un-Friend My Heart* ibid.

<sup>48</sup> Gershon, *Un-Friend My Heart* ibid.

### 3.3 TECHNICAL USE

Answers to most technical questions about Facebook can be found by navigating Facebook's Help Center.<sup>49</sup> I will, however, give an overview of Facebook's most commonly used features. When signing up for Facebook, the only information that is required is one's first name, last name, email address, sex, birthday (including date, month, and year), and a password. The only information that requires any form of confirmation is your email address.<sup>50</sup> Beyond this information, all information that is provided to and posted on Facebook is at the discretion of the user. This leaves open the possibility for the creation of fake accounts (an issue to be discussed later).

#### 3.3.1 USER PROFILE

Facebook begins with a user 'Profile.' Profiles are unique pages where one can "type oneself into being."<sup>51</sup> The profile is where other Facebook users look to find information about a Facebook user. Beyond stating the name of the user, all Facebook profiles have what is called a 'Profile Picture.' Facebook provides a default silhouette photo, but almost all users replace this photo with one of their choosing. On each person's profile page, a small version of one profile picture (chosen by the user) is displayed, but if a user

---

<sup>49</sup> Facebook "Help Center" online: <<http://www.facebook.com/help/>>.

<sup>50</sup> Upon registration, a confirmation email is sent to the email address provided with a link for activation of the account.

<sup>51</sup> See Boyd and Ellison, *Social Network Sites: Definition, History, and Scholarship*, *supra* at note 40, 211.

clicks on the picture, a bigger, clearer version of the picture (and past profile pictures) is accessible. In addition to the user's name and profile picture, every profile has certain 'tabs.' Tabs are categorizations of information that is contained in a user profile. I will now describe each of these tabs.

### **3.3.1.1 INFO**

As can be inferred from the title of this tab, this is where information about the user can be found. Such information can include (but is not limited to) the following<sup>52</sup>: sex, relationship status (including specifics of the relationship i.e. the identity of significant other), employer and job status, religion, education, "people who inspire me", favourite quotations, favourite TV shows, favourite books, favourite movies, sports I play, favourite sports teams, favourite athletes, activities and interests, email address, phone number, address, hometown, current city, and languages spoken. In addition to this, there is a slot titled "about me," where a user can write something about himself or herself that is not captured by the other categories.

### **3.3.1.1 NOTES**

Notes is a tab that allows a facebook user to write a note. This is akin to a 'blog,' in that it is a space where someone can write whatever they wish for people to read.

---

<sup>52</sup> This is the information that a user is prompted, but not required, to share by Facebook.

### **3.3.1.1 PHOTOS**

The Photos tab is exactly what it sounds like it would be. Under this tab are pictures associated with this user profile. Users can upload pictures to their profile by creating what is called an “album.” Albums are given a title, and each photo in the album has a space for the uploading user to write a caption for the specific photo. The time and date that the picture is uploaded is also displayed with every picture.<sup>53</sup>

Photos can also be uploaded to a user’s profile through the use of the “tagging” feature. I will explore this feature in more detail below.

### **3.3.1.1 FRIENDS**

The Friends tab displays all of a user’s “friends” on Facebook. People become friends in the following way. User X comes across user Y’s profile. At the top of user Y’s profile is an “add friend” button. If user X clicks that button, a friend request will be sent to user Y. User Y then has the option to ‘confirm’ or ‘ignore’ user X’s request. If user Y confirms, then they become friends; if user Y ignores, they do not become friends. The Friends tab will show all of a user’s friends. Under this tab there is also an option for “family,” which shows which users you are related to, and the specific nature of that familial relation.

---

<sup>53</sup> The date and time of all facebook posts is indicated by the time zone of the user on whose profile the information is posted.



Under the friends tab there is also a clustering of that user's friends who you share as "mutual friends." These are users who are friends with both you and that user.

### **3.3.1.1 WALL**

The wall is a virtual whiteboard where the user and the user's friends can post messages. Wall posts indicate the author of the message by displaying the user's name<sup>54</sup> next to the post. It also includes the date and time the author posted the message. Wall posts can be in the form of text, hyperlink, or a photo. Wall posts are time-stamped.

### **3.3.2 STATUS UPDATE**

In the status update bar is the following question: "What's on your mind?" This is where users can write what is similar to a wall post; however, it is posted onto your own wall. Status updates can be in the form of text, hyperlink, a photo, or a video. Status updates are also time-stamped.

### **3.3.3 TAGGING**

Tagging a user in something adds that user's name to a post in the form of a hyperlink, in that it can be clicked and the clicker can be brought directly to user's profile. Users can be tagged in notes, wall posts, status

---

<sup>54</sup> In a hyperlink form, so the name can be clicked to be directed to the user's profile.

updates, photos, and videos. When a user is tagged in something, not only does their name appear in that post, but the post also appears on the person's profile. When a user is tagged in a photo, not only does the user's name appear in hyperlink form with the photo, but when the cursor hovers over the tagged user name, an indication appears on the photo itself identifying who the tagged user is.

Another form of tagging is what is known as "checking in." A user can write a status update about where they are, and can tag the location. This can be done using GPS from a mobile phone, or the location will have its own Facebook page that can be tagged into the post.

### **3.3.4 NEWS FEED**

In 2006, Facebook launched the "News Feed."<sup>55</sup> When a user logs into Facebook, they are immediately brought to his or her news feed. As the Facebook homepage, the news feed operates as a type of news ticker that instantly informs the user of any of his or her friends' activity. For example, if a friend changes his or her profile picture, writes a status update, or posts a photo album, this activity will show up in the news feed. Only the activity of a user's friends shows up in the user's news feed. User friends' birthdays are also displayed on the Facebook homepage beside the news feed. It is possible

---

<sup>55</sup> Ruchi Sangvhi, "Facebook Gets a Facelife" *The Facebook Blog* (5 September 2006) online: <<http://blog.facebook.com/blog.php?post=2207967130>>

for users to customize their news feed in such a way that updates about certain friends do not show up in the news feed.

### **3.3.5 MESSAGES**

Besides wall posts, Facebook users can communicate with one another in a more private forum – messages. Messages are akin to emails in that they are sent from one user to another user, and are only accessible in the users’ inboxes. Messages can be between two users, or many users. Each Facebook user has a “Messages” tab on the Facebook site that is accessible only by the user. Each correspondence between users shows up in a “thread” detailing the history of the correspondence. For example, if user X and user Y have an ongoing correspondence, either user, under their messages tab, would have a history of their correspondence treated as one correspondence. Only those two could access the correspondence. However, if user X and user Y and user Z had a message correspondence between the three of them, it would be treated as a correspondence separate from user X and user Y’s correspondence, and all three users could access the history of the correspondence between users X, Y, and Z. All messages are time-stamped.

### **3.3.6 COMMENTING**

Another way people communicate is by commenting on other user’s (or the user’s own) activity. Whether it is a photo, status update, note, or wall post, a user’s friend can comment on the post. Such comments show up in the news feed along with the post

itself, and are viewable not only by the user who posted the note, but also that user's friends. All comments are time-stamped.

### **3.3.7 THE "LIKE" BUTTON**

Like comments, users can "Like" other users' posts. For example, if user X posted something (a photo, status update, wall post, etc.), and user Y clicked the "Like" button below the post, then a message below the post that says "user Y likes this" will appear below the post. All who can see the post can see who liked the post. Likes are not time-stamped, but they would have to have happened after the post itself, which is time-stamped. While the wording of "liking" implies that the clicking user liked the activity, this is not always the case and because it is a type of electronic 'rubber stamp' that cannot be altered, what is meant by a "like" can vary depending on the circumstances.

### **3.3.8 CHAT**

Another forum/form of communication between users is through Facebook chat. When a user is logged into Facebook on a computer, there is an application called chat, where the user can see what other users are "online"<sup>56</sup> and the user's can engage in instant messaging. A log of the chat history is kept in the messages tab as a form of message correspondence between the users. All messages sent are time-stamped. Users can select to not appear "online" in chat, despite being logged into Facebook.

---

<sup>56</sup> Meaning they are also using the chat application at that time.

In the chat application there is also the option to have a video chat, using your computer's webcam. Such conversations are not logged into the correspondence thread under the messages tab.

### **3.3.9 EVENTS**

Events are pages that are created for future events that are happening, either online or in the physical world. Event pages are much like user profiles in that they have a wall, information tab, and photos. Users create the event page, give the event a title, and provide the time, date, place, picture, and a description. Users are then invited to the event and can RSVP by clicking either "Attending," "Not Attending," or "Maybe." It is then displayed on the event page itself who is attending, who is not, and who is a "maybe." If a user is attending an event, a notification will show up on the user's profile, and in the user's friends' news feed.

### **3.3.10 GROUPS**

Groups, like events, are created by Facebook users and have their own page. Facebook groups, like social groups, can be about pretty much anything – from fans of a certain TV show to members of a bridge club to cycling enthusiasts in Halifax. In the group, members can make wall posts, create discussion topics, and post pictures and videos. Groups are places for people with similar interests to congregate to discuss a subject matter of shared interest.

### **3.3.11 PAGES**

Pages are similar to profiles, but they often represent a certain cause. Many businesses, organizations, celebrities, and social causes have their own Facebook page. Like groups, there can be a page for almost anything. A page is like a profile, in that it looks essentially the same as a profile, only pages do not have friends. Pages post updates for people to see. To have these updates show up in your News Feed, a user is to “like” the page, much the same way they “like” a post by a friend. It is displayed on each page how many people “like” the page, much like on user’s profiles where it displays who a user’s friends are. When a user likes a page, not only do they subscribe to the page’s updates, but a notification of this “like” shows up on the user’s profile and the news feeds of the user’s friends. When one creates a Page, he or she is agreeing to the possibility of his or her Page being “liked” by anyone – there is no confirmation process as there is for a friend request.

### **3.3.12 SEARCH BAR**

At the top of every page of Facebook is a toolbar. On this toolbar there is a search bar where a user can search for friends, users who are not friends, groups, pages, events, etc. There are also other parts of Facebook (profile, messages, newsfeed etc.) that are accessible through the toolbar, but the search bar is located only on the toolbar at the top of the page.

### **3.3.13 POKES**

On each user's profile there is an option to "poke" the user. When one user pokes another, the user who was poked receives a notification of the poke, and who it is from. Much like a "like," it is not known what exactly a poke means.

### **3.3.14 NOTIFICATIONS**

When a Facebook user does something on Facebook that involves you, you receive what is called a "notification." There will be a notice on the site telling you what happened, whether it is a wall post, a photo tag, a friend request, or when someone "likes" or comments on one of your posts. There is also an option to receive notifications via email or text message to a user's phone. Notifications are received instantly when the activity occurs, and are time-stamped.

### **3.3.15 TIMELINE**

Recently, Facebook profiles, while keeping the same features, have been reorganized into what is known as a "Timeline." Content on a regular profile appears in sequential order, starting with the most recent. Under this set-up, to view a user's activity from months or years ago, depending on the frequency of that user's activity, it was necessary to scroll through a lot of information in search of something in particular. With timeline, all activity is organized along a clickable timeline, allowing viewers to click back to a certain year or month in search of activity. Something new that comes along with a Timeline is what is called a "Cover Photo." The Cover Photo is a type

of banner that sits at the top of a user's Profile. The user does not need to have a Cover Photo, but should he or she choose to, he or she can upload any picture he or she wishes as his or her Cover Photo.

### **3.3.16 SEE FRIENDSHIP**

Below an interaction between two users is a "see friendship" link. Clicking this link brings the viewer to a page that details the interactions between the two users, as well as any mutual events, groups, tagged photos, etc. that those two users share.

### **3.3.17 FACEBOOK MOBILE**

Virtually all that can be done via the Facebook website can also be done via Mobile application on a smartphone.

## **3.4 PERSONAL INFORMATION**

What all of these Facebook features and applications add up to is a record of the user's activity, and given the plethora of ways in which users can interact and share on Facebook, to track the user's activity can reveal some of the most intimate details of a person's life. George Washington University law professor Orin Kerr has said that asking for access to someone's social networking information is "akin to requiring someone's



house keys.”<sup>57</sup> I submit that the information that a person can potentially access logging into another’s Facebook account is even more invasive than entering the person’s home. All the information is filed, organized, and can be easily navigated by those who know where to look – it can provide a complete digital mapping of the user’s life both in the form of black and white text, as well as digital photos. The information that can be found out can pertain to, but is not limited to, personal preferences, religious beliefs, relationships, interests, personal correspondences, health, hobbies, employment information (and the list can go on); essentially, it can reveal some of the most intimate aspects of an individual’s life. Daniel Solove has written the following about the collection of personal digital information:

Digital technology enables the preservation of the minutia of our everyday comings and goings, of our likes and dislikes, of who we are and what we own. It is ever more possible to create an electronic collage that covers much of a person’s life – a life captured in records, a digital person composed in the collective computer networks of the world.<sup>58</sup>

With this in mind, Facebook allows its users to select their own privacy settings for their online activity.

### **3.5 FACEBOOK PRIVACY**

---

<sup>57</sup> *The Sydney Morning Herald* “It’s Akin to Requiring Someone’s House Keys: Employers Ask Job Seekers For Facebook Passwords” (21 March 2012) online: <<http://www.smh.com.au/technology/technology-news/its-akin-to-requiring-someones-house-keys-employers-ask-job-seekers-for-facebook-passwords-20120321-1vioi.html>>

<sup>58</sup> Daniel Solove, *The Digital Person: Technology and Privacy in the Information Age*, (New York: NYU Press 2004) at 1 [*The Digital Person*].

Mark Zuckerberg has been quoted as saying that “the problem Facebook is solving is this one paradox...People want access to all the information around them, but they also want control of their own information. Those two things are at odds with each other. Technologically, we could put all the information out there for everyone to see, but people wouldn’t want that because they want to control their information.”<sup>59</sup> As a result of this paradox, the privacy settings for a user’s content are, for the most part, under the control of the user. Not just in the sense that the user is the generator of the activity, but also in the sense that Facebook allows the user to configure who can see the content they put on Facebook. It is unequivocally stated in Facebook’s Principles<sup>60</sup>, Data Use Policy<sup>61</sup>, and Statement of Rights and Responsibilities<sup>62</sup> that the Facebook user owns their own information; however, it is also acknowledged that Facebook does use this information for their own purposes (i.e. advertising, troubleshooting, to make suggestions to users, etc.). Each type of Facebook interaction can have different privacy settings. For example, your status updates can have one privacy setting, and your tagged photos can have a different privacy setting. There are a few default privacy setting that Facebook suggests to a user.

---

<sup>59</sup> Gershon, *Un-Friend My Heart supra* at note 45.

<sup>60</sup> Facebook “Principles” online: <<http://www.facebook.com/principles.php>>.

<sup>61</sup> Facebook “Data Use Policy” online:  
<<http://www.facebook.com/about/privacy/>>.

<sup>62</sup> Facebook “Statement of Rights and Responsibilities” online:  
<<http://www.facebook.com/legal/terms>>.

### **3.5.1 PUBLIC**

Under this setting, all activity is viewable by anyone on Facebook, and your profile page and its contents are even accessible to anyone with access to a web browsing service, regardless of whether he or she is a Facebook member or your friend. This is the least private privacy setting on the site; rather, it could be more appropriately characterized as a “lack of privacy” setting, as it makes your Facebook activity available to everyone. Currently, the only aspect of Facebook that has to remain completely public is a user’s Cover Photo, should the user choose to have one.

### **3.5.3 FRIENDS AND NETWORK**

This allows your content to be viewed by your friends, as well as anyone who is a member of your “Network.” A Network is some kind of community, often a town or school, to which people belong. Under this setting, all of your friends, and all Facebook members of that network can view your content.

### **3.5.3 FRIENDS AND FRIENDS OF FRIENDS**

This allows your content to be viewed by your friends, as well as anyone who is a friend of one of your friends.

### **3.5.4 FRIENDS**

This setting makes your content viewable to only your friends.

### **3.5.4 CUSTOM**

This setting is, as the name would suggest, customizable. This is potentially the most private setting possible. The least private a custom setting can be is that the content is viewable by friends, friends of friends, and those users in your network. However, it is possible to customize the privacy settings in your content so that it is only viewable by certain groupings of friends, or perhaps viewable by all friends except a certain few, or even viewable by only you, the user of the account. The custom privacy settings allow a user to contour which Facebook users can view what content, and to what extent. It is the most elaborate privacy setting possible. To illustrate, while it would defeat the interactional purpose of Facebook, under the custom setting, it is possible to make all of your content viewable only by yourself and either the author of the post, or the person who is on the receiving end of anything you post (i.e. a wall post).

Users have their default settings made to whatever setting they choose; however, there is a clickable option beside each post that is known as the “audience selector.” The audience selector is a dropdown box that allows the user to select privacy settings for each item he or she posts, thus making the privacy settings for every single post he or she makes customizable before it is posted. As a result, while the content generated by a user is being put

onto Facebook, there are varying degrees of expectations with respect to the coded privacy that protects the specific content and its accessibility to other Facebook users.

Also, it is possible to block another Facebook user. Doing this makes it so that user cannot see any of your Facebook activity and you cannot see any of his or her activity. From that user's perspective, it is as if you are not on Facebook.

### **3.6 ACTIVITY LOG**

From a user's profile, there is a clickable "Activity Log" that details all of a user's Facebook activity that is viewable by others on Facebook. Here, there will be a time stamped timeline of any new friendships, comments, uploads, "likes," etc. It also shows who the possible audience for the particular activity is based on the receiving user's privacy settings.

### **3.7 FAKE ACCOUNTS AND LOGIN INFORMATION SHARING**

Given how easily a Facebook page can be created, and how easily login information can be shared between individuals, Facebook's Statement of Rights and Responsibilities explicitly prohibits the practices of creating fake accounts and sharing your login information. Section 4(1) stipulates that "You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission." Section 3 (5)

stipulates that “You will not solicit login information or access an account belonging to someone else.” Section 4 (1) stipulates that “You will not share your password...let anyone else access your account, or do anything else that might jeopardize the security of your account.” These parts of the Statement of Rights and Responsibilities serve to provide some solace to Facebook users in that they can feel comfortable that the content he or she posts on the site is, at least according to the Statement of Rights and Responsibilities, viewable only by those users whom they have deemed to have access to his or her posts.

With that said, it is still very possible and simple to create a fake Facebook account. In fact, Facebook recently reported in a form 10-Q filing with the United States Securities and Exchange Commission that there are 83 million fake Facebook accounts.<sup>63</sup> According to the report, those 83 million accounts make up 8.7% of total accounts on Facebook; of that 8.7%, 4.8% are duplicate accounts, 2.4% are user-misclassified accounts, and 1.5% are spam.<sup>64</sup> Furthermore, while the aforementioned agreements between Facebook and its users prevent login information sharing, the reality is that

---

<sup>63</sup> Todd Wasserman, “83 Million Facebook Accounts Are Fake” *Mashable Social Media* (2 August 2012) online: <<http://mashable.com/2012/08/02/fake-facebook-accounts/>> [83 Million Facebook Accounts Are Fake]. 10-Q file available at <[http://www.sec.gov/Archives/edgar/data/1326801/000119312512325997/d371464d10q.htm#tx371464\\_14](http://www.sec.gov/Archives/edgar/data/1326801/000119312512325997/d371464d10q.htm#tx371464_14)>.

<sup>64</sup> 83 Million Facebook Accounts Are Fake, *ibid.*

it is extremely easy for individuals to pass along their login information to others, allowing multiple people to have access to a single Facebook account.

### **3.8 USE OF FACEBOOK**

How exactly a particular user uses his or her Facebook account depends on the user. One way that Facebook can be used is simply to keep in touch with friends. It has advantages in this regard that are not available via email, in that people can keep in touch in various degrees. Unlike email, where one can only send messages (with attachments, hyperlinks, other media), on Facebook, the medium (i.e. private message, wall post, comment, “like,” etc.) is part of the message. In this regard, the way a Facebook account is used can be very nuanced depending on the relationship between the users.

Something else unique that Facebook allows is for individuals to have a virtual space that they can shape both in content and audience in order to put out a clear picture, using a multitude of mediums, of who they believe themselves to be. People can customize, alter, or change their Facebook page instantly depending on their own personal preferences. This allows for individuals to present a sense of self in a very easy and convenient way – this is a major value of Facebook.

### **3.9 “CREEPING”**

On the other side of the coin, something for which Facebook use is particularly notorious, is what has become known as “creeping.” Creeping involves perusing through another user’s profile, including their pictures, wall posts, statuses, etc. The subject of a user’s Facebook creeping may be the user’s friend, but depending on the subject’s privacy settings, he or she may not be the friend of the user who is creeping. All Facebook users, by virtue of signing up for the service are openly inviting creeping to varying degrees, depending on their privacy settings. Essentially, Facebook interaction and communication is not considered creeping, but simply looking through anyone’s Facebook profile is, and it is considered to be especially “creepy” to look through a person’s Facebook profile if he or she is not your friend. Creeping is, for all intents and purposes, undetected monitoring of a user’s Facebook activity. A vital aspect of Facebook that allows for creeping is that it in no way makes available the information or the extent to which one user views another user’s profile.

### **3.10 PRIVACY COMMISSIONER ISSUES**

Facebook has on more than one occasion been the subject of reviews by the Office of the Privacy Commissioner of Canada. The Office of the Privacy Commissioner of Canada has been investigating Facebook almost continuously since 2009. It used to be such that not all elements of a user’s Facebook account had customizable privacy settings (i.e. all users could see



certain elements of a Facebook profile, regardless of whether they were a user's Friend). As a result, Privacy Commissioner Jennifer Stoddart has twice issued reports that have urged Facebook to ramp up users' ability to control the privacy settings on more aspects of their Facebook account and make the language of user agreements and the ability to customize privacy settings more clear and user-friendly.<sup>65</sup> It is important to note here that the aim of the Privacy Commissioner's reports was to allow people more control in their ability to select their audience. This is very much in keeping with the discussion of the meaning of privacy protection in Chapter 2 – privacy protection is not about being left alone, but rather about the ability of individuals to have a sense of control when it comes to choosing their audience for different parts of their lives.

All Privacy Commissioner reports resulted in Facebook agreeing to take active steps with a view towards complying with the Privacy Commissioner's requests. While the specifics of these reports are not entirely pertinent to this work, the constant monitoring and alteration in the name of

---

<sup>65</sup> See the following news releases from the Office of the Privacy Commissioner of Canada: "Facebook agrees to address Privacy Commissioner's concerns" (27 August 2009 (online): <[http://www.priv.gc.ca/media/nr-c/2009/nr-c\\_090827\\_e.asp](http://www.priv.gc.ca/media/nr-c/2009/nr-c_090827_e.asp)>; "Privacy Commissioner launches new Facebook probe" (27 January 2012) online: <[http://www.priv.gc.ca/media/nr-c/2010/nr-c\\_100127\\_e.asp](http://www.priv.gc.ca/media/nr-c/2010/nr-c_100127_e.asp)>; "Privacy Commissioner completes Facebook review" (22 September, 2012) online: <[http://www.priv.gc.ca/media/nr-c/2010/nr-c\\_100922\\_e.asp](http://www.priv.gc.ca/media/nr-c/2010/nr-c_100922_e.asp)>; "Privacy Commissioner: Facebook shows improvement in some areas, but should be more proactive on privacy when introducing new features" (4 April 2012) online: <[http://www.priv.gc.ca/media/nr-c/2012/nr-c\\_120404\\_e.asp](http://www.priv.gc.ca/media/nr-c/2012/nr-c_120404_e.asp)>.

privacy protection demonstrates that the nature of the use of Facebook as a form of online socializing presents significant issues when it comes to the legal protection of privacy.

## CHAPTER 4      The Current Landscape of Canadian Privacy Law

The primary mechanism for protection of individuals' privacy interests is specific privacy legislation. Given the inherent privacy issues that arise through the use of Facebook, the focus of this Chapter will be to examine the current landscape of privacy legislation in Canada. In particular, this Chapter will outline the relevant provisions of certain pieces of Canadian privacy legislation that pertain to social networking information in the context of the employment relationship and examine where the legislation falls short. Finally, this Chapter will explore the new Canadian tort of "intrusion upon seclusion."

Privacy legislation exists at both the federal and provincial levels, and there are different pieces of legislation regulating the public sector and the private sector. The federal *Privacy Act*<sup>66</sup> regulates any collection or use of personal information by the federal government and agencies of the federal government in the public sector. There also exists in most provinces privacy legislation to regulate collection and use of personal information by the provincial government and agencies of the provincial government in the public sector. The *Personal Information Protection and Electronic Documents Act* [*PIPEDA*]<sup>67</sup> is federal legislation that applies to every organization in respect of personal information that the organization collects, uses, or

---

<sup>66</sup> RSC 1985, c P-21 [*Privacy Act*].

<sup>67</sup> SC 2000, c 5 [*PIPEDA*]

discloses in the course of commercial activities; <sup>68</sup> – this is the privacy legislation that applies to the federally regulated private sector. It also purports to apply to provincially regulated industries, but only with respect to a business’s commercial activities – not their employment relationships.<sup>69</sup> Some provinces have also enacted provincial private sector privacy statutes that regulate private institutions that fall under provincial jurisdiction – provinces are acknowledged under section 26(2)(b) of *PIPEDA* as having authority to enact legislation that the federal government agrees will replace *PIPEDA*, so long as that legislation is found to be substantially similar to *PIPEDA*. This has been done in Alberta and British Columbia. As such, there is a Memorandum of Understanding among The Office of the Privacy Commissioner of Canada, The Office of the Privacy Commissioner of Alberta, and the Office of the Privacy Commissioner of British Columbia with respect to cooperation and collaboration in private sector privacy policy, enforcement, and public education.<sup>70</sup> This agreement is not a result of delegation from the federal to the provincial, but based on the assumption that both the federal

---

<sup>68</sup> *PIPEDA*, *ibid* at s 4(2)(a).

<sup>69</sup> The constitutionality of *PIPEDA*’s application to provincially regulated industries is a potentially contested issue. The argument in favour of federal jurisdiction rests upon the Trade and Commerce power in s 91(2) of the *Constitution Act, 1867*, 30 & 31 Vict, c 3, in light of trade dictates by the European Union.

<sup>70</sup> See Provincial and Territorial Privacy Commissioners and Ombuds Office, “Memorandum of Understanding” (November 2011) online: <[http://www.priv.gc.ca/au-ans/mou\\_e.asp](http://www.priv.gc.ca/au-ans/mou_e.asp)>.

and provincial Offices have concurrent and overlapping jurisdiction in these matters.<sup>71</sup>

While not the focus of this work, there also exist several federal and provincial sector-specific privacy laws.

I will now examine the provisions of the aforementioned statutes that could apply to an individual's social networking content in the context of the employment relationship.

#### **4.1 PRIVACY ACT**

The *Privacy Act* is federal legislation that came into effect on July 1<sup>st</sup>, 1983. The *Act* sets out rules as to how the federal government must treat and handle the personal information of individuals. "Personal Information" is defined, under the *Act*, as information about an identifiable individual recorded in any form, and the *Act* lists specific examples of what is included, without restricting the generality of the definition.<sup>72</sup> The *Act* applies to federal government institutions, which, under the *Act*, are defined as (1) any department or ministry of state of the Government of Canada or any body or office located in the *Act's* schedule, as well as (b) any parent Crown Corporation, and any wholly-owned subsidiary of such a corporation.<sup>73</sup> The *Act* imposes limitations on what can be collected by a government institution,

---

<sup>71</sup> As mentioned *supra* at note 69, the propriety of federal jurisdiction is a contested issue.

<sup>72</sup> *Privacy Act, supra* at note 66, s 3.

<sup>73</sup> *Privacy Act, ibid.*

how it can be collected, and for what purposes. Section 4 stipulates that no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution.<sup>74</sup> According to section 5 (1)(2), any information that is collected must, wherever possible, be collected directly from the individual and the individual must be made aware of the purpose(s) for which the information is being collected.<sup>75</sup> There are, however, exceptions to these requirements – if compliance may result in the collection of inaccurate information, or defeat the purpose or prejudice the use for which the information is collected, the requirements of section 5(1)(2) do not apply.<sup>76</sup> The requirement of collection directly from the individual also does not apply if the individual authorizes an alternate form of collection. Under the *Act*, every individual has the right to request and be given access to the personal information about the individual under the control of the government institution that is reasonably retrievable, and if the information is inaccurate, the individual has the right to request correction of any information that is not accurate.<sup>77</sup> Any complaints under the *Act* are to be heard and investigated by the Privacy Commissioner of Canada.<sup>78</sup>

---

<sup>74</sup> *Privacy Act, ibid* at s 4.

<sup>75</sup> *Privacy Act, ibid* at s 5(1)(2).

<sup>76</sup> *Privacy Act, ibid* at s 5(3).

<sup>77</sup> *Privacy Act, ibid* at s 12.

<sup>78</sup> *Privacy Act, ibid* at s 29.

What does this mean for an employer collecting the social networking information about a job candidate or an employee? It means that if the employer is a federal government institution, it may only collect social networking information about a job candidate or employee if that information relates directly to an operating program or activity of that federal government institution. This is fairly restrictive. Not only this, but (with some limited exceptions) the individual must be made aware of the collection prior to the collection, must consent to the collection, and wherever possible, the institution must collect this information directly from the individual.

#### **4.2 PROVINCIAL PUBLIC SECTOR PRIVACY LEGISLATION**

All provinces<sup>79</sup> have enacted legislation that regulates the collection, use, and disclosure of personal information by provincial governments in the public sector.<sup>80</sup> While not exactly uniform across jurisdictions, their standard for collection of information is essentially the same as in the *Privacy Act* – the

---

<sup>79</sup> *An Act Respecting access to Documents Held by Public Bodies and the Protection of Personal Information*, RSQ, c A-2.1; *Freedom of Information and Protection of Privacy Act*, SS 1990-91, c F-22.01; *Freedom of Information and Protection of Privacy Act*, RSA 2000, c F-25 [FIPPA AB]; *Freedom of Information and Protection of Privacy Act*, SNS 1993, c 5 at s 24(1) [FIPPA NS]; *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165; *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31; *The Freedom of Information and Protection of Privacy Act*, CCSM c F175; *Right to Information and Protection of Privacy Act*, SNB 2009, c R-10.6; *Freedom of Information and Protection of Privacy Act*, SNS 1993, c 5; *Freedom of Information and Protection of Privacy Act*, RSPEI 1988, c F-15.01; *Access to Information and Protection of Privacy Act*, SNL 2002, c A-1.1.

<sup>80</sup> Michael Power et al, “Access to Information and Privacy” *Halsbury’s Laws of Canada* (2011 Reissue) online at HAP-62 (QL) [Access to Information and Privacy].

collection of the information must relate directly to and be necessary for an operating program or activity of the public body.<sup>81</sup> These pieces of legislation apply to public sector institutions under the authority of the provincial government, and they define personal information broadly, providing an illustrative and extensive list of what constitutes “personal information;” social networking information would certainly fall within the definition of personal information under all provincial Acts.<sup>82</sup> Consent is required in all cases (with certain limited exceptions), though the form consent must take is not defined in the statutes of Manitoba, New Brunswick, Nova Scotia, Newfoundland and Labrador, or Ontario.<sup>83</sup> With certain exceptions, personal information is to be collected directly from the individual.<sup>84</sup> Under all provincial Acts, there is an obligation on the institution to take steps to ensure the information is accurate.<sup>85</sup> Standards similar to those in the *Privacy Act* exist under provincial privacy legislation for the use and disclosure of the information that was collected.

What this all amounts to is that there exist substantially similar levels and standards of privacy protection for the provincial public sector as there are for the federal public sector.

---

<sup>81</sup> See, for example, *FIPPA AB*, *supra* at note 79 at s 3, *FIPPA NS*, *supra* at note 79 at s 24(1).

<sup>82</sup> Access to Information and Privacy, *supra* at note 80, HAP-54.

<sup>83</sup> Access to Information and Privacy, *ibid* at HAP-53.

<sup>84</sup> Access to Information and Privacy, *ibid* at HAP-63; an exception to this is *FIPPA NS*, *supra* at note 79, which does not require direct collection.

<sup>85</sup> Access to Information and Privacy, *ibid* at note 80, HAP-72.



### **4.3 PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS Act [PIPEDA]**

*PIPEDA* is federal legislation that came into effect on April 13<sup>th</sup>, 2000. “Personal Information” is defined under *PIPEDA* as information about an identifiable individual, but does not include the name, title, or business address or telephone number of an employee of an organization.<sup>86</sup> Social networking activity and information would certainly fall within this definition of personal information.

The types of organizations and information that *PIPEDA* regulates are set out in section 4(1). There is some trickiness to its application. It states that *PIPEDA* applies to every organization in respect of personal information that it (a) uses, collects, or discloses in the course of commercial activities; or (b) is about an employee of the organization and that the organization uses, collects, or discloses in connection with the operation of a federal work, undertaking, or business.<sup>87</sup> An “organization” is defined as including but not limited to an association, partnership, person or a trade union.<sup>88</sup> It is explicitly stated *PIPEDA* does not apply to those organizations that fall under the purview of the *Privacy Act* – so it does not apply to any federal government institutions.<sup>89</sup> “Commercial Activities” are defined as any

---

<sup>86</sup> *PIPEDA*, *supra* at note 67, s 2.

<sup>87</sup> *PIPEDA*, *ibid* at s 4(1).

<sup>88</sup> *PIPEDA*, *ibid* at s 2.

<sup>89</sup> *PIPEDA*, *ibid* at s 4(2).

particular transaction, act, or conduct or any regular course of conduct that is commercial in character.<sup>90</sup> “Employee” is not defined under s. 2. Section 27.1(3) states that “employee” is to include independent contractors, but it is also explicitly stated that this is for the purpose of s. 27.<sup>91</sup> While they are not necessarily identical across the board, it can be assumed that for the purposes of the application of *PIPEDA*, employee is to be given a standard definition, similar to the ones that it is given in the common law and under employment standards legislation, or trade union or labour relations legislation.<sup>92</sup> With respect to *PIPEDA*’s application to an employee, section 4(1) means that if an organization is federally regulated (i.e. radio broadcasting, inter-provincial trade, a bank, etc.<sup>93</sup>), *PIPEDA* applies to employee information. However, if an organization is not federally regulated, *PIPEDA* only applies to employee information that is used in a commercial way (i.e. selling the information to a marketing company). This means that *PIPEDA* does not apply to employee information collected by organizations that are not federally regulated, so long as that information is not used in a commercial way. To be clear, unless it is collected for some commercial

---

<sup>90</sup> *PIPEDA*, *ibid* at s 2.

<sup>91</sup> S 27’s purpose is to say that no employer shall dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee for complying with the provisions of *PIPEDA*. As a result, this explicit definition does not apply in the context of an employee’s social networking information.

<sup>92</sup> The statutory definition of “employee” for employment standards legislation will be further explained in Chapter 5.

<sup>93</sup> See “Federal work, undertaking, or business” in *PIPEDA*, *supra* at note 67, s 2.

purpose, social networking information collected about an employee by a private sector employee working in a provincially regulated industry is not protected under *PIPEDA*. This is the result of Canada's constitutional division of powers. There is an argument for the federal government, as a result of its jurisdiction over trade and commerce, to have jurisdiction over privacy issues for commercial activities normally under provincial jurisdiction; however that same argument cannot be made for the employment relationship itself.

*PIPEDA* allows collection, use, and disclosure of personal information only for purposes that a reasonable person would consider appropriate in the circumstances.<sup>94</sup> Except where "inappropriate," the organization is required to notify and obtain consent from the individual if the information the organization intends to collect, use, or disclose is about that individual.<sup>95</sup> "Inappropriate" circumstances include situations where legal, medical, or security reasons make it impossible or impractical to seek consent.<sup>96</sup> The purpose of the collection of information must be identified before the collection, and the actual collection must be limited to that identified purpose unless the individual consents otherwise.<sup>97</sup> The individual is free to

---

<sup>94</sup> *PIPEDA*, *ibid* at s 5(3).

<sup>95</sup> *PIPEDA*, *ibid* at Schedule I, 4.3.

<sup>96</sup> Also, s 7(1)(a) allows for collection of information if its collection is in the interest of the individual, but the individual's consent cannot be obtained in a timely manner.

<sup>97</sup> *PIPEDA*, *supra* at note 67, Schedule I 4.4 and 4.5.

withdraw his or her consent at any time.<sup>98</sup> The organization is under an obligation to take steps to ensure that all information it collects is accurate, and the individual who is the subject of said information has a right to request and gain access to the information and ask for corrections of inaccurate information.<sup>99</sup>

What does this mean for an employer collecting the social networking information about a job candidate or an employee? It means that if the employer is a private sector institution working in a federally regulated industry, they may only collect social networking information about a job candidate or employee if that collection is done for purposes that would be considered reasonable in the circumstances. This is not as restrictive as the *Privacy Act* – the only restriction on the information that is collected is that it be done for “reasonable” purposes. It is not clarified whether this standard is the “reasonable employer” or the “reasonable employee;” just that the purposes of collection be reasonable. Substantially, the same requirements for consent, prior notification, and direct collection that apply to the *Privacy Act* apply to *PIPEDA*.

#### **4.4 PROVINCIAL PRIVATE SECTOR PRIVACY LEGISLATION**

As was mentioned above, provincial legislatures are acknowledged under section 26(2)(b) of *PIPEDA* as having the authority to enact legislation

---

<sup>98</sup> *PIPEDA*, *ibid* at Schedule I 4.3.8.

<sup>99</sup> *PIPEDA*, *ibid* at Schedule I 4.6.

that the federal government agrees will replace *PIPEDA*, so long as that legislation is found to be substantially similar to *PIPEDA*. Thus far, the only provinces that have done so are Quebec, British Columbia, and Alberta.<sup>100</sup> In all three of these provinces, the enactment of these statutes goes beyond what *PIPEDA* does for provincially regulated businesses, in that its scope is not limited to personal information collected for the commercial transactions. While Quebec's legislation<sup>101</sup> provides privacy protection similar to that provided by *PIPEDA*, something unique to the provincial statutes in Alberta and British Columbia is that they have separate definitions of "personal information" and "employee personal information/personal employee information," and standards of collection, as well as certain requirements for the collection process differ depending whether the information being collected is deemed to be "personal information" or "employee personal information/personal employee information".

#### **4.4.1 PERSONAL INFORMATION PROTECTION ACT OF BRITISH COLUMBIA [PIPA BC]**

---

<sup>100</sup> Ontario has adopted such privacy legislation; however, the *Personal Health Information Protection Act*, 2004, SO 2004, c 3, Sch A pertains only to the protection of personal health information.

<sup>101</sup> *An Act Respecting the Protection of Personal Information in the Private Sector*, RSQ, chapter P-39 1 [*PPIPS QUE*]. One notable difference is at s 5, where the standard for collection of personal information is that "Any person collecting personal information to establish a file on another person or to record personal information in such a file may collect only the information necessary for the object of the file." This standard does not seem very restrictive at all.

The stated purpose of *PIPA BC*<sup>102</sup> is to “govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of individuals to protect their personal information and the need of organizations to collect, use or disclose personal information that a **reasonable person** would consider appropriate.”<sup>103</sup> (emphasis added) *PIPA BC* applies to every “organization,” which is defined as including a person, unincorporated association, a trade union, a trust or a not for profit organization, and it also lists some exclusions – one of which is “a public body.”<sup>104</sup> This is to say that organizations that fall under *The Privacy Act*, or any provincial equivalent do not fall under the purview of *PIPA BC*. “Personal Information” is defined as information about an identifiable individual, and includes employee personal information, but does not include contact information or work product information.<sup>105</sup> Section 6 of *PIPA BC* provides that subject to some exceptions, no personal information is to be collected, used, or disclosed unless the individual gives consent.<sup>106</sup> Furthermore, prior to collecting the information, the organization is required to disclose to the individual the purposes for which the information is collected.<sup>107</sup> The individual may withdraw their consent at any time,<sup>108</sup> and if

---

<sup>102</sup> SBC 2003 c 63 [*PIPA BC*].

<sup>103</sup> *PIPA BC*, *ibid* at s 2.

<sup>104</sup> *PIPA BC*, *ibid* at s 1.

<sup>105</sup> *PIPA BC*, *ibid* at s 1.

<sup>106</sup> Exceptions to this are in ss. 12, 15, and 18.

<sup>107</sup> *PIPA BC*, *supra* at note 102, s 10(1)(b).

<sup>108</sup> *PIPA BC*, *ibid* at s 9(1).

he or she does, the organization must 1) inform the individual the likely consequences of withdrawing his or her consent,<sup>109</sup> and 2) must stop the collection, use, or disclosure of the individual's personal information.<sup>110</sup> Finally, the actual collection has to be limited to information that a reasonable person would consider appropriate in the situation and that fulfill the purposes that the organization disclosed to the individual whose information is being collected.<sup>111</sup> This definition of personal information most certainly includes social networking information; however, when the information being collected is the social networking information of a job candidate or an employee, it is classified as a different type of information – “employee personal information.”

With respect to employee personal information, *PIPA BC* has very different standards. “Employee Personal Information” is personal information about an individual that is collected, used, or disclosed for the purposes reasonably required to establish, manage, or terminate an employment relationship, but it does not include personal information that is not about the individual's employment. An organization can collect employee personal information without the individual's consent;<sup>112</sup> however, before that collection is carried out, the organization must inform the individual that it

---

<sup>109</sup> *PIPA BC, ibid* at s 9(2).

<sup>110</sup> *PIPA BC, ibid* at s 9(4).

<sup>111</sup> *PIPA BC, ibid* at s 11.

<sup>112</sup> *PIPA BC, ibid* at s 13(1).

will be collecting the information and the purposes for the collection.<sup>113</sup> The same standards apply for the use of employee personal information<sup>114</sup>, and disclosure of employee personal information.<sup>115</sup> This is an important difference with all of the privacy legislation discussed above, as they all require consent before the collection, use, or disclosure of personal information (with certain exceptions). The only standard for what employee personal information can be collected without consent is that the collection be reasonable for the purposes of establishing, maintaining, or terminating an employment relationship.

What does this mean for an employer collecting the social networking information about a job candidate or an employee? It means that if the employer is a private sector institution in British Columbia, they may only collect social networking information about a job candidate or employee if the collection of that information is reasonable for employment purposes (establishing, maintaining, terminating). This is essentially the same standard as *PIPEDA*, only it makes specific reference to the information's relevance in the employment context. Another important distinction is that under *PIPA BC*, unlike all of the privacy legislation discussed thus far, the employee or candidate does not need to consent to the collection of said information.

---

<sup>113</sup> *PIPA BC*, *ibid* at s 13 (3).

<sup>114</sup> *PIPA BC*, *ibid* at s 16.

<sup>115</sup> *PIPA BC*, *ibid* at s 19.



#### **4.4.2 PERSONAL INFORMATION PROTECTION ACT OF ALBERTA [PIPA AB]**

The stated purpose of *PIPA AB*<sup>116</sup> is to govern the collection, use, and disclosure of personal information by organizations in a manner that recognizes both the right an individual has to have his or her personal information protected and the organization's need to collect, use, and disclose personal information for reasonable purposes.<sup>117</sup> Section 4 of *PIPA AB* states that it applies to every organization and in respect to all personal information, and it lists some exceptions.<sup>118</sup> One such exception, like *PIPA BC*, is any public body – meaning organizations that fall under the purview of the *Privacy Act* or any provincial equivalent. An “organization,” under *PIPA AB* includes a corporation, an unincorporated association, a trade union, a partnership, and an individual acting in a commercial capacity, but does not include an individual acting in a personal or domestic capacity.<sup>119</sup> “Personal Information” is defined as any information about an identifiable individual. According to section 7(1), an organization may not collect, use, or disclose an individual's personal information unless the individual consents to the collection, use, or disclosure.<sup>120</sup> Furthermore, the organization is required to

---

<sup>116</sup> SA 2003 c P-6.5 [*PIPA AB*].

<sup>117</sup> *PIPA AB*, *ibid* at s 3.

<sup>118</sup> *PIPA AB*, *ibid* at s 4.

<sup>119</sup> *PIPA AB*, *ibid* at s 1(i).

<sup>120</sup> This is subject to certain exceptions. See *PIPA AB*, *ibid* at ss 14, 17, and 20.

collect the information directly from the individual unless the individual consents to the information being collected from another source.<sup>121</sup> Prior to or on collecting the information, the organization must disclose to the individual the purposes of the collection.<sup>122</sup> An individual may withdraw or vary his or her consent to the collection, use, or disclosure of the personal information.<sup>123</sup> Upon receipt of notice, the organization must inform the individual of the consequences of such a withdrawal or variation,<sup>124</sup> and in the case of a withdrawal of consent, stop collecting, using, or disclosing information,<sup>125</sup> and in the case of a variation of consent, abide by the consent as varied.<sup>126</sup> The information that can be collected by an organization is limited to information that is used for reasonable purposes, and only to the extent that is reasonable for meeting the purposes for which the information is collected.<sup>127</sup> As is the case with *PIPA BC*, social networking falls under the *PIPA AB*'s definition of personal information; however, when it comes to information about an employee or job candidate, there is a different definition of personal information with different standards.

“Personal Employee Information” is personal information about an individual who is a potential, current, or former employee of an organization

---

<sup>121</sup> *PIPA AB*, *supra* at note 116, s 7(1)(b).

<sup>122</sup> *PIPA AB*, *ibid* at s 13.

<sup>123</sup> *PIPA AB*, *ibid* at s 9(1).

<sup>124</sup> *PIPA AB*, *ibid* at s 9(2).

<sup>125</sup> *PIPA AB*, *ibid* at s 9(4)(a).

<sup>126</sup> *PIPA AB*, *ibid* at s 9(4)(b).

<sup>127</sup> *PIPA AB*, *ibid* at s 11.

that is reasonably required by the organization for the purposes of 1) establishing, managing, or terminating an employment relationship, or 2) managing a post-employment relationship, but does not include information that is unrelated to that relationship.<sup>128</sup> Personal employee information can be collected without the consent of the individual if it is collected solely for the purposes of establishing, managing, or terminating an employment relationship between the organization and the individual.<sup>129</sup> If, however, the individual is a current employee, he or she must be informed that the information will be collected, and the purposes of its collection; however, it is not necessary that the employee consent.<sup>130</sup> The same standard is used for the use<sup>131</sup> and disclosure<sup>132</sup> of personal employee information. The only standard that applies to the collection of personal employee information is that it be reasonable to collect that information.<sup>133</sup> These are essentially the same standards as *PIPA BC*.

On the following two pages is a table delineating the applicable variations among the statutes discussed in this chapter.

---

<sup>128</sup> *PIPA AB, ibid* at s 1(j).

<sup>129</sup> *PIPA AB, ibid* at s 15(1)(a).

<sup>130</sup> *PIPA AB, ibid* at s 15(1)(c).

<sup>131</sup> *PIPA AB, ibid* at s 18(1).

<sup>132</sup> *PIPA AB, ibid* at s 21(1).

<sup>133</sup> *PIPA AB, ibid* at s 15(1)(b).

**4.5 TABLE 1**

	<u>Privacy Act</u>	<u>Provincial Public Sector Privacy Legislation</u>	<u>PIPEDA</u>	<u>PPIPS Que</u>	<u>PIPA AB</u> <u>PIPA BC</u>
*Denotes Varies slightly					
<b>Application to Employees' Information</b>	Federal Government and Federal Public Sector	Provincial Government and Provincial Public Sector	Private Organizations in Federally Regulated	Private Organizations in Quebec	Private Organizations in Alberta/BC
<b>Requirement of Consent? (with exceptions)</b>	Yes	*Yes	Yes	Yes	No
<b>Must Inform Prior (with exceptions)</b>	Yes	Yes	Yes	Yes	Yes
<b>Withdraw Consent?</b>	Yes	Yes	Yes	Yes	Not Applicable
<b>Requirement of Direct Collection (with</b>	Yes	Yes	Yes	Yes	Not Applicable
<b>Requirement To Ensure Accuracy</b>	Yes	Yes	Yes	Yes	Yes

*Denotes Varies slightly	<u>Privacy Act</u>	<u>Provincial Public Sector Privacy Legislation</u>	<u>PIPEDA</u>	<u>FIPPS Que</u>	<u>PIPA AB</u> <u>PIPA BC</u>
<b>Type of Information</b>	Information about an identifiable individual in any form	Recorded information about an identifiable individual *	Information about an identifiable individual, but not the name, title, or business address or telephone number of an employee of an organization	Any information which relates to a natural person and allows that person to be identified.	Information about an individual who is a potential, current, or former employee of an organization to establish, manage, or terminate an employment relationship, or managing a post-employment relationship*
<b>Standard for Information</b>	Information must relate directly to the operation or program	Information must relate directly to the operation or program*	Information that a reasonable person would consider appropriate in the circumstances	Information collected for a file on a person may only be information necessary for the object of that file	Information must be reasonably required for employment purposes

As can be seen in the table above, the legislation is fairly uniform across the board, with some important differences that can present significant discrepancies in privacy protection depending which statute applies to the information in question. The legislation governing the public sector has more stringent requirements as to what information can be collected compared with the legislation regulating the private sector. Two outliers are *PIPA BC* and *PIPA AB* with their qualified standards for information relating to employment, and do not require consent prior to collection.

## **4.6 THE TORT OF INVASION OF PRIVACY**

### **4.6.1 TORT CREATED BY STATUTE**

British Columbia, Saskatchewan, Newfoundland and Labrador, and Manitoba have created a statutory cause of action for invasion of privacy when a person without a claim of right<sup>134</sup> willfully violates the privacy of another.<sup>135</sup>

---

<sup>134</sup> “Claim of right” in this context has been defined as an honest belief in a state of facts, which, if it existed, would be a legal justification or excuse – see *Access to Information and Privacy*, *supra* at note 80, HAP-258.

<sup>135</sup> *The Privacy Act*, CCSM c P125 [*Privacy Act MB*]; *Privacy Act*, RSS 1978, c P-24 [*Privacy Act Sask*]; *Privacy Act*, RSBC 1996, c 373 [*Privacy Act BC*]; *Privacy Act*, RSNL 1990 c-P22 [*Privacy Act NL*].

These statutes have only been judicially considered to a very limited extent, and courts do not find readily in favour of a plaintiff.<sup>136</sup> The nature and degree of privacy to which an individual is entitled is that of what is reasonable in the circumstances,<sup>137</sup> and the relationship between the plaintiff and the defendant is a relevant consideration.<sup>138</sup> However, it has been found that no invasion of privacy can occur where the plaintiff has consented to the act or conduct in question.<sup>139</sup> As a result, the impact of this legislation on protection afforded to the collection of social networking information in the employment context is minimal. What it amounts to is that in BC, Manitoba, Newfoundland and Labrador, and Saskatchewan, employers may need consent to collect an employee's social networking information, if collecting that information is not reasonable in the circumstances. And given the fact that *PIPA BC* does not even require consent prior to collecting such information, it is unlikely that to collect said information without consent would be considered unreasonable in the circumstances.

Outside of British Columbia, Alberta, Manitoba, Saskatchewan, Quebec, and Newfoundland and Labrador there is one group of employees

---

<sup>136</sup> Access to Information and Privacy, *supra* at note 80, HAP-258.

<sup>137</sup> See, for example, *Privacy Act AB*, *supra* at note 116, s 4(2)(b).

<sup>138</sup> See *Pierre v Pacific Press Ltd*, [1994] B.C.J. No. 583 (BCCA).

<sup>139</sup> See *Walker v British Columbia College of Dental Surgeons*, [1997] BCJ No 433 (BCSC); *Cottrell v Manitoba (Workers Compensation Board)* [1997] MJ No 249 (Man QB); and *K (SJ) v Chapple*, [1999] SJ No 186, (Sask QB).

that do not seem to have the benefit of any legislated privacy protection whatsoever – employees or potential employees working in the private sector for companies that conduct business in industries that are regulated by a provincial government. These employers do not seem to fall under the purview of any of privacy legislation. As a result, there is no legislated privacy protection for these employees or job candidates, and the only place these people can find privacy protection with respect to their social networking activity can be found in the common law.

#### **4.6.2 RIGHT TO PRIVACY AT COMMON LAW**

In *Somwar v McDonald's Restaurants of Canada*,<sup>140</sup> Justice Stinson first expressed that the time has come for the court to recognize the tort of invasion of privacy. In *Somwar*, the defendant conducted a credit background check on the plaintiff (who was an employee of the defendant) without the permission of the plaintiff. While acknowledging that Ontario law was unsettled as to whether a common law tort of invasion of privacy could exist, Stinson wrote that

with advancements in technology, personal data of an individual can now be collected, accessed (properly and improperly), and disseminated more easily than ever before. There is a resulting increased concern in our society about the risk of unauthorized access to an individual's personal information. The traditional torts such as nuisance, trespass, and harassment may not provide adequate protection against infringement of an individual's privacy interests. Protection of those privacy

---

<sup>140</sup> [2006] OJ No 64 [*Somwar*].



interests by providing a common law remedy for their violation would be consistent with Charter values and an "incremental revision" and logical extension of the existing jurisprudence<sup>141</sup>

In *Somwar*, it was not necessary for Justice Stinson to reach a conclusion whether the tort of invasion of privacy should be recognized by the court<sup>142</sup>; however, Stinson's decision proved to be the first step that eventually led to the groundbreaking decision of the Ontario Court of Appeal in *Jones v Tsige*.<sup>143</sup>

Squarely at issue in *Jones* was whether there exists a tort for invasion of privacy. Jones and Tsige worked at the same branch of the Bank of Montreal.<sup>144</sup> Jones did not know Tsige, but Tsige was in a common-law relationship with Jones's ex-husband.<sup>145</sup> Over the course of a four-year period, Tsige used her workplace computer to access Jones's banking records at least 174 times.<sup>146</sup> The records included financial information, as well as personal information; Tsige did not publish, distribute, or record the information – she only looked through it.<sup>147</sup> Jones became suspicious and complained to her employer, and

---

<sup>141</sup> *Somwar*, *ibid* at paragraph 29.

<sup>142</sup> This was a decision on a motion brought by the defendant seeking to dismiss the plaintiff's action on the ground that the statement of claim discloses no reasonable cause of action.

<sup>143</sup> *Jones*, *supra* at note 26.

<sup>144</sup> *Jones*, *ibid* at paragraph 4.

<sup>145</sup> *Jones*, *ibid* at paragraph 4.

<sup>146</sup> *Jones*, *ibid* at paragraph 4.

<sup>147</sup> *Jones*, *ibid* at paragraph 4.

when asked about it, Tsige admitted to her actions, said she had no legitimate reason for looking at Jones's records, acknowledged it was a violation of BMO's code of conduct, and apologized for her actions; BMO disciplined Tsige by suspending her for a week without pay and denying her a bonus.<sup>148</sup> Jones sued Tsige, asserting that her privacy interest in her banking records had been irreversibly destroyed, claimed damages of \$70,000 for invasion of privacy, as well as punitive and exemplary damages of \$20,000; Jones's action was dismissed on the ground that the tort of invasion of privacy did not exist.<sup>149</sup> Jones appealed the decision to the Ontario Court of Appeal.

In a unanimous decision of a three-member panel, the Court of Appeal allowed Jones's appeal and awarded \$10,000, stating that, "it is appropriate for this court to confirm the existence of a right of action for intrusion upon seclusion. Recognition of such a cause of action would amount to an incremental step that is consistent with the role of this court to develop the common law in a manner consistent with the changing needs of society."<sup>150</sup> So, the new tort of "intrusion upon seclusion" was born in Canadian law. In defining the tort, Justice Sharpe cited the following classification by Professor Robert Prosser that has been adopted by the American *Restatement (Second) of Torts*

---

<sup>148</sup> *Jones, ibid* at paragraphs 5-6.

<sup>149</sup> *Jones v Tsige*, [2011] OJ No 1273.

<sup>150</sup> *Jones, supra* at note 26, paragraph 65.

(2010): “One who intentionally intrudes, physically or otherwise, upon the seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the invasion would be highly offensive to a reasonable person.”<sup>151</sup>

In coming to his decision, Justice Sharpe wrote extensively about the importance of the legal protection of privacy, and the threat that technological advancement poses to that threat. From paragraphs 66-69, Justice Sharpe writes the following:

The case law, while certainly far from conclusive, supports the existence of such a cause of action. 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. The right to informational privacy closely tracks the same interest that would be protected by a cause of action for intrusion upon seclusion. Many legal scholars and writers who have considered the issue support recognition of a right of action for breach of privacy...

For over one hundred years, technological change has motivated the legal protection of the individual's right to privacy. In modern times, the pace of technological change has accelerated exponentially. Legal scholars ... have written of "the pressing need to preserve 'privacy' which is being threatened by science and technology to the point of surrender" ... The internet and digital technology have brought an enormous change in the way we communicate and in our capacity to capture, store and retrieve information. As the facts of this case indicate, routinely kept electronic databases render our

---

<sup>151</sup> *Jones, ibid* at paragraph 19.

most personal financial information vulnerable. Sensitive information as to our health is similarly available, as are records of the books we have borrowed or bought, the movies we have rented or downloaded, where we have shopped, where we have travelled, and the nature of our communications by cell phone, e-mail or text message.

It is within the capacity of the common law to evolve to respond to the problem posed by the routine collection and aggregation of highly personal information that is readily accessible in electronic form. Technological change poses a novel threat to a right of privacy that has been protected for hundreds of years by the common law under various guises and that, since 1982 and the Charter, has been recognized as a right that is integral to our social and political order.

Adopting the formulation for “intrusion upon seclusion” that is set out in the American *Restatement of Torts*, Justice Sharpe explicitly set out the elements of the tort as “first, the defendant’s conduct must have been intentional, within which I would include reckless; second, that the defendant must have invaded, without lawful justification, the plaintiff’s private affairs or concerns; and third, that a reasonable person would regard the invasion as highly offensive causing distress, humiliation, or anguish.”<sup>152</sup> However, it was unequivocally stated that while proof of economic harm or harm to economic interests is not an element of the tort, given the intangible nature of privacy interests, damages for the tort will be a “modest conventional sum.”<sup>153</sup> The

---

<sup>152</sup> *Jones, ibid* at paragraph 71.

<sup>153</sup> *Jones, ibid* at paragraph 71.

creation of this new tort in *Jones* has been recognized in decisions in jurisdictions outside of Ontario.<sup>154</sup>

It should be noted that Justice Sharpe found that the privacy interest at stake here was classified as “informational privacy,” which was defined as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”<sup>155</sup> The implications of such a categorization of privacy will be discussed in greater detail in Chapter 8.

What this exploration of the landscape of Canadian privacy law shows is that the degree of privacy afforded to an individual’s social networking information can vary greatly depending on the location and industry in which they are working or seeking to find a job. The next Chapter will explore how these privacy protections actually work, or fail to work, to protect an individual’s social networking information in the pre-employment phase – when an individual is seeking a job.

---

<sup>154</sup> See *Trout Point Lodge Ltd v Handshoe* [2012] NSJ No 427 at paragraph 35; *BDC v BJB* [2012] YJ No 91 at paragraph 19.

<sup>155</sup> *Jones, supra* at note 26, paragraph 41.

## CHAPTER 5      Application to the Pre-Employment Phase

Given the plethora of information that can be found on an individual's Facebook account, many employers have incorporated "creeping" as part of their candidate-vetting process. An emerging trend in the hiring process is what is called a social networking background check. What this amounts to is looking into the prospective employee's social networking activity to gain a fuller picture of who the candidate is and what they are like. According to a March 2010 survey, 90 percent of employment recruiters said they used web search engines to research candidates, and 46 percent said that they ruled candidates out on that basis.<sup>156</sup> According to a 2009 survey, as many as 45 percent of respondents used social networking background checks as a tool for screening candidates.<sup>157</sup> Social networking background checks can vary case-by-case in terms of their degree of intrusion upon the private affairs of the candidate – it range anywhere from a "Google" search of the candidate's name, to requesting the candidate to "friend" the

---

<sup>156</sup> The survey, conducted by ExecuNet Executive Insider March 2010, was republished by Meg Montford, "Why #Jobseekers MUST Manage Their Online Reputation" *Career Chaos* (1 March 2010) online: <[http://coachmeg.typepad.com/career\\_chaos/2010/03/why-jobseekers-must-manage-online-reputation.html](http://coachmeg.typepad.com/career_chaos/2010/03/why-jobseekers-must-manage-online-reputation.html)>.

<sup>157</sup> Rosemary Haefner, "More Employers Screening Candidates via Social Networking Sites" *Careerbuilder* (10 June 2009) online: <<http://careerbuilder.com/Article/CB-1337-Getting-Hired-More-Employers-Screening-Candidates-via-Social-Networking-Sites/>>.

employer or a human resources staff member on Facebook<sup>158</sup>, to requesting that the candidate login to Facebook from a company computer during the interview.<sup>159</sup> Some employers even go so far as to request a candidate's login information and password during the interview itself so they can peruse the candidate's Facebook account.<sup>160</sup> There even exist businesses that offer social networking background checks as a service to employers who wish to find out more about the candidates that they interview.<sup>161</sup>

The reason an employer would want to look at a candidate's social networking content is fairly obvious. Hiring an employee can be a very important decision, and the potential cost of hiring the wrong employee can be significant; as was mentioned in previous Chapters, social networking accounts can be a very fertile source of information into the personality and lifestyle of an individual. An employer can gain a certain personal insight about an individual and his or her lifestyle that

---

<sup>158</sup> Information and Privacy Commissioner (Ontario), *Reference Check: Is Your Boss Watching? The New World of Social Media: Privacy and Your Facebook Profile* (April 2012), online: <<http://www.ipc.on.ca/images/Resources/facebook-refcheck.pdf>> at p 4 [*Reference Check*].

<sup>159</sup> *Reference Check*, *ibid* at p 5.

<sup>160</sup> Morgan Campbell, "Would you reveal your Facebook password for a job?" *The Toronto Star* (20 March 2012) online: <<http://www.thestar.com/business/article/1148973--would-you-reveal-your-facebook-password-for-a-job>>.

<sup>161</sup> For example, American companies include Social Intelligence, Sterling InfoSystems, InfoCheckUSA, and Tandem Select, and a Canadian company is CSI-Screening.

may not be so easily retrievable through resumes, cover letters, reference checks, or even face-to-face conversations. For these reasons, it is understandable why an employer may want to delve into a prospective employee's social networking information.

In the United States, an employer looking through a job candidate's social networking information may not be doing so out of curiosity or a wish to find the right "fit"; as a result of the tort of "Negligent Hiring," an employer may even argue that he or she is legally obligated to perform such background checks on potential employees.<sup>162</sup> The doctrine of negligent hiring imposes upon employers liability for harm caused to third parties by the employer's employee; however, it is different from vicarious liability in that the liability can be imposed regardless of whether the employee was acting within his or her capacity as an employee.<sup>163</sup> Liability will be imposed when an employer "places an unfit person in an employment situation that entails an unreasonable risk of harm to others."<sup>164</sup> The primary focus in determining liability is to examine the adequacy of the employer's pre-employment investigation into the employee's background.<sup>165</sup> While

---

<sup>162</sup> Robert Sprague, "Rethinking Information Privacy in an Age of Online Transparency" (2008) 25 Hofstra Lab & Empl J 395 at 398 [*Rethinking Information Privacy*].

<sup>163</sup> *Rethinking Information Privacy*, *ibid* at 398.

<sup>164</sup> Rosanne Lienhard, "Negligent Retention of Employees: An Expanding Doctrine" (1996) 63 Def Couns J 389 at 389.

<sup>165</sup> *Rethinking Information Privacy*, *supra* at note 162 398.



this is an American tort, it is entirely possible that just like intrusion upon seclusion, negligent hiring makes its way into Canadian tort law. It is certainly not a stretch to think that a situation in which an unreasonable risk is created for others as a result of hiring a person who is unfit for an employment situation could be covered by existing negligence principles in Canadian tort law.<sup>166</sup> Consequently, it gives employers another reason to find out all they can about a candidate prior to offering them employment. However, if the determination of liability comes down to the adequacy of the employer's investigation into the candidate's background, the issue becomes the extent to which an employer should reasonably be expected to investigate the candidate's background. In Chapter 8, I will explore, in the context of social networking information, the extent to which it should be permissible for an employer to delve into the affairs of a job candidate. While I will be

---

<sup>166</sup> See Allen Linden, Bruce Feldthusen et al, "Negligence" *Halsbury's Laws of Canada*, (2012) online (QL) at HNE-2, where the following six-part examination for when a cause of action for negligence arises. 1) The claimant must suffer some damage; 2) The damage suffered must be caused by the conduct of the defendant; 3) The defendant's conduct must be negligent, that is, in breach of the standard of care set by law; 4) There must be a duty recognized by the law to avoid this damage; 5) The conduct of the defendant must be a proximate or legal cause of the loss or, stated in another way, the damage should not be too remote as a result of the defendant's conduct; 6) The conduct of the plaintiff should not be such as to bar or reduce recovery, that is, the plaintiff must not be guilty of contributory negligence and must not voluntarily assume the risk. Under this test, it is not difficult to contemplate a situation in which an employer's failure to adequately investigate the background of a job candidate amounts to negligence on the part of the employer.

exploring the extent to which such a background check should be limited, this should give an indication as to the degree of social networking background check that an employer should be reasonably expected to conduct.

Indeed, these social networking background checks give rise to some new legal issues. This Chapter will examine the way Canadian law works (or does not work) to address these issues.

## **5.1 APPLICATION OF EMPLOYMENT STANDARDS LEGISLATION**

As mentioned in Chapter 2, each province has legislation that substantively regulates the employment relationship within that province. For the most part, these Acts apply to employers and employees. These pieces of legislation do not use uniform wording in defining an “employee.” Typical definitions under the Acts include such persons as follows: an individual employed to do work who receives or is entitled to wages,<sup>167</sup> a homemaker,<sup>168</sup> and a person who receives training from the employer or the employer’s business.<sup>169</sup> Despite the wording not being uniform across the board, for the most part, the substance of who is considered to be an “employee” under provincial employment standards legislation is broadly similar. Definitions of “employer” in Employment Standards legislation, while also not

---

<sup>167</sup> *Employment Standards Code*, RSA 2000, c E-9 s 1(1)(k).

<sup>168</sup> *Employment Standards Act*, SO 2000 c 41 s 1(1).

<sup>169</sup> *Employment Standards Act*, RSBC 1996 c 113 s 1(1).

uniform, tend to include persons who are responsible for the payment of wages to employees,<sup>170</sup> and a person who has control or direction of an employee.<sup>171</sup>

While the steps that lead up to the creation of the employment contract are critical to the employment relationship itself, definitions of employee and employer under these Acts do not appear to pertain to the pre-employment phase. The only situation in which a prospective employee receives any protection under Employment Standards legislation is with respect to lie detector tests in Ontario and New Brunswick.<sup>172</sup> Outside of this context, prospective employees do not receive any protection from Employment Standards legislation until they enter into an employment contract with the employer. As a result, it would appear that any legal issues arising from a social networking background check, despite the fact that they pertain directly to the creation of an employment contract, do not fall under the ambit of any Employment Standards legislation.

In the provisions of the New Brunswick and Ontario Employment Standards legislation referred to above, no employer is permitted to request that a prospective employee submit to a lie detector test. This is thought provoking. It is safe to assume that the reason for these

---

<sup>170</sup> *Labour Standards Act*, RSS 1979 c L-1 s 2 (e).

<sup>171</sup> *Employment Standards Act*, RSBC, *supra* at note 169, s 1(1).

<sup>172</sup> *Employment Standards Act*, SO, *supra* at note 170, s 68 and *New Brunswick Employment Standards Act*, SNB 1982, c E-7.2 s 44.1(1).

provisions is the product of the intrusive nature and inherent unreliability of lie detector tests. It is not a stretch to draw an analogy here between a lie detector test and certain forms of social networking background checks, especially when all an employer asks for is a candidate's login name and password – to look through a candidate's Facebook account in this way is both extremely intrusive, and it would be very difficult for the employer to be able discern the accurate social networking information from that which is unreliable.

## **5.2 DEGREES OF INVASIVENESS**

At this point I think it is useful to list what I consider to be the differing degrees of invasiveness in social networking background checks. I divide them into three levels of invasiveness and label them as (1) password, (2) public, and (3) 'in-between'.

### **5.2.1 PASSWORD**

The type of social networking background check that I label "password" has the highest level of invasiveness. In this type of background check, the employer requests (or requires) the candidate's social networking login information and password, and explores the candidate's social networking account on his or her own. During such a search, it is virtually certain that the employer will come across irrelevant

information, information from third parties, and there certainly exist alternatives to this search to retrieve only information that a reasonable person would consider appropriate in the circumstances. It is my position that such a background check should be deemed inappropriate in any pre-employment circumstance.

### **5.2.2 PUBLIC**

The type of social networking background check that I label “public” has the lowest level of invasiveness. In such a background check, the employer looks only at the candidate’s social networking information that is publicly available – meaning the information that the candidate does not have under any privacy protection and can be found via a Google or Facebook search. While such a background check could still very likely lead to collection of irrelevant information, and such information could potentially form the basis of a privacy or human rights complaint (to be discussed below), I would contend that by making the information completely accessible to the public, the candidate is consenting to the possibility of the information being at least seen by anyone with access to the internet.<sup>173</sup>

### **5.2.3 IN-BETWEEN**

---

<sup>173</sup> I am not, however, saying that the candidate is consenting to a particular use of the information, only that it may be seen by potential employers.

The type of social networking background check that I label “in between” is the trickiest. It could range from the employer requesting (or requiring) to be ‘Friends’ with the candidate to requesting that the candidate login to his or her social networking site and navigate certain parts of his or her account while the employer looks on. The invasiveness of the background check depends on the nature of the background check, and in the In-Between category, the candidate has at least some level of control as to what the employer will see (through privacy settings), or direct knowledge of what the employer has seen (if they are present for the background check). Whether the background check in this category should be allowed will depend on a case-by-case basis. This will be further explored in Chapter 8.

### **5.3 A RISK FOR EMPLOYERS: HUMAN RIGHTS**

Given the sheer volume and depth of information contained on a social networking profile and account, employers who delve into the social networking information of a candidate set themselves up for a potential human rights violation. The *Canadian Human Right Act* prohibits refusing to employ and discriminate a candidate on the basis of a prohibited ground.<sup>174</sup> Provincial human rights statutes have

---

<sup>174</sup> *Canadian Human Rights Act*, RSC 1985 c H-6 s 7. The prohibited grounds referred to in s 7 can be found in s 3(1) and include race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital status, family status, disability and conviction for an offence for

similar provisions.<sup>175</sup> Facebook profiles, whether accessed via Google search, as a “friend,” or by logging into the user’s account, almost all contain information that could fall within one of the prohibited grounds of discrimination.

Under the “Application for Employment” heading, the *Ontario Human Rights Code* provides as follows:

The right under section 5 to equal treatment with respect to employment is infringed where a form of application for employment is used or a written or oral inquiry is made of an applicant that directly or indirectly classifies or indicates qualifications by a prohibited ground of discrimination.<sup>176</sup>

In commenting about what this provision of the *Code* means for the employment application phase, Professor David Doorey has written the following:

Section 23(2) says that an employer can’t ask a job applicant for information that “directly or indirectly” classifies a person by a prohibited ground. In other words, it is none of an employer’s business if you are married or single (family status), whether you are gay, straight, or bisexual (sexual orientation), what your religion is (creed) or your race, if you are Aboriginal, what your skin colour is, where you are from, how old you are, whether you have children (family status), and whether you have a disability. Some of these things will be evident by the interview stage (like skin colour and maybe disability), but the employer certainly cannot ask you to disclose other information about prohibited

---

which a pardon has been granted or in respect of which a record suspension has been ordered.

<sup>175</sup> See, for example, *Ontario Human Rights Code*, RSO 1990, c H.19 s 5(1).

<sup>176</sup> *Ontario Human Rights Code*, *ibid* at s 23(2).

grounds that are not self-evident in the interview.

Moreover, Section 23 doesn't just ban the question "Are you disabled?", it bans other questions that are likely to give the employer the answer to that question, such as "Can you lift 50 pounds and stand for extended periods of time?". The objective is to keep information about the applicant's association with prohibited grounds out of the hands of employers during the recruitment stage.<sup>177178</sup>

As previously stated, Facebook profiles, whether accessed via Google search, as a "friend," or by logging into the users account, almost all contain information that could fall within one of the prohibited grounds of discrimination. The Ontario Human Rights Commission issued a statement (on Facebook) saying that employers should not engage in the practice of asking job applications for access to information on their social networking sites and that doing so could open them up to a claim of discrimination.<sup>179</sup>

---

<sup>177</sup> David Doorey, "Can an Employer ask a Job Applicant for their Facebook Password?" *Doorey's Workplace Law Blog: Thoughts on Canadian Labour & Employment Law for Students & Others* (20 March 2012) online: <<http://www.yorku.ca/ddoorey/lawblog/?p=4995>>.

<sup>178</sup> It should also be mentioned here that an employer can ask questions about what are known as *Bona Fide Occupational Requirements* [BFORs], for example, asking someone seeking a position as a priest in an Anglican Church if they are Anglican; see *British Columbia (Public Service Employee Relations Commission) v. British Columbia Government and Service Employees' Union (B.C.G.S.E.U.)* [1999] S.C.J. No. 46.

<sup>179</sup> Ontario Human Rights Commission, "Statement regarding employers asking for Facebook passwords," (23 March 2012) online: <<https://facebook.com/the.orhc/posts/320570581329371>>.



While Professor Doorey is of the opinion that accessing a candidate's Facebook page could be a violation of the *Ontario Human Rights Code*, the language of s. 23(2) only refers to the classification of a candidate by a prohibited ground; it seems to be concerning the *use* of the content found in the candidate's social networking information – not the *viewing* (or collection) of the information. This is an important distinction. In order for a human rights complaint to be successful, the applicant would need to prove that the employer *used* the information on the site to classify the applicant based on a prohibited ground – this would be very difficult. While showing that the employer had access to the social networking contents does raise suspicion, it proves only that there was access – it proves nothing with respect to how the employer actually used the information, or whether it played any part in an employer classifying the candidate based on a prohibited ground of discrimination. The reality of the situation is that, for the most part, those who are put in charge of the hiring process make the actual hiring decisions behind closed doors. If the basis for which a candidate is not chosen is actually based upon information found in his or her social networking content (and pertains to a prohibited ground of discrimination), a prudent employer who is mindful of a potential human rights action would not openly state that this is the reason the candidate was not hired – so long as there exist other, plausible reasons,

the employer will likely cite those. Absent some concrete disclosure from the employer about how they used the information, or the candidate somehow obtaining a copy of an internal memo or email written to that effect, a candidate launching human rights complaint based on the employer's access to his or her social networking content would encounter great difficulty in terms of proof.<sup>180</sup> As a result, the practical efficacy of human rights legislation to address this practice is minimal. And while employers certainly do, in reality, open themselves up to the possibility of violating human rights legislation by looking into a candidate's social networking content, absent some slip up on their part in terms of disclosure to the applicant, they can rest easy that it would be very difficult for a complainant candidate to make out a case under human rights law as it currently stands.

#### **5.4 ANOTHER RISK FOR EMPLOYERS: UNFAIR LABOUR PRACTICES**

The employer is in no way in direct control of what a job candidate has written in his or her Facebook account, nor does the employer have any indication that something may or may not be written on a candidate's Facebook account until the employer makes specific

---

<sup>180</sup> I am not saying proof here is impossible – there does exist the possibility that the employer has a history of discriminatory practices that may make their alternate explanation look suspect. However, my general point is that a cautious employer can circumvent the statute with relative ease, and, as a result, the effectiveness of the protection afforded by the legislation is compromised.

explorations to find out. As a result, it is entirely possible that a job candidate has something on his or her Facebook account that would lead a reader to believe that he or she is in some capacity a supporter of workers' unions. Upon discovering this, an employer has put himself or herself in a very tricky situation, as discriminating in the hiring process upon that basis would be commission of an unfair labour practice.<sup>181</sup> Here, however, the same problems exist as in human rights matters – unless there is some kind of disclosure on the part of employer, it would be difficult to prove that this was the reason the employer decided not to hire the candidate. However, with an allegation of such an unfair labour practice, the onus rests on the employer to prove that he or she did not commit an unfair labour practice.<sup>182</sup> This makes it more difficult for an employer to circumvent the legislation; if an employer has a history of anti-union animus, his or her alternate explanation for the hiring decision will be looked at with more scrutiny.

#### **5.4 SPECIFIC LEGISLATION**

In Nova Scotia, a Liberal MLA has introduced a Private Member's Bill that seeks – similar to the lie detector prohibition in New Brunswick and Ontario – to prohibit an employer from requiring an employee or prospective employee to provide the employer with access

---

<sup>181</sup> See *Labour Relations Act*, R.S.N.L. 1990, c. L-1, s. 24(1); *Trade Union Act*, R.S.S. 1978, c. T-17, s. 11(1)(e).

<sup>182</sup> See, for example, *Trade Union Act*, RSNS 1989, c 475 at s 56(3).

to his or her social networking account or discriminating against the employee or prospective employee for refusing to provide access to his or her social networking account.<sup>183</sup> The proposed Bill states that an employer shall not require the password or related account information for the purpose of gaining access to the person's account,<sup>184</sup> demand access in any manner to a person's account,<sup>185</sup> or penalize, in any way, a person because he or she refused to comply with such a request.<sup>186</sup> It is important to note that an employer is not prohibited, under the Bill, to obtain information that is in the public domain – meaning that only social networking information that is under some sort of privacy protection via the website falls under the ambit of the Bill.<sup>187</sup> The Nova Scotia government is currently considering the Bill. Similar legislation currently exists in a handful of American states, and the United States Senate is considering similar legislation at the federal level.<sup>188</sup>

---

<sup>183</sup> Bill No. X (as introduced), *An Act to Amend Chapter 246 of the Revised Statutes, 1989, the Labour Standards Code*, 4<sup>th</sup> Session, 61<sup>st</sup> General Assembly, Nova Scotia, 61 Elizabeth II, 2012, Private Member's Bill, Andrew Younger, MLA for Dartmouth East [*Bill No X*].

<sup>184</sup> *Bill no X, ibid* at s 2(a).

<sup>185</sup> *Bill no X, ibid* at s 2(b).

<sup>186</sup> *Bill no X, ibid* at s 3.

<sup>187</sup> *Bill no X, ibid* at s 4.

<sup>188</sup> Tina Giesbrecht and Roland Hung, "Are Employers in British Columbia and Alberta stepping outside privacy boundaries in requesting access to a job applicant's social media profile?" *McCarthy Tetrault Publications* (5 April 2012) online: <[http://www.mccarthy.ca/article\\_detail.aspx?id=5814](http://www.mccarthy.ca/article_detail.aspx?id=5814)>.

It is important to note that unlike the lie detector provisions in New Brunswick and Ontario, the only focus of this Bill is to prohibit the demanding or requiring that an employee or potential employee give the employer access to his or her social networking site (and penalizing the employee or potential employee for refusing to do so). This is to say that while the Bill does prevent an employer from *requiring* either login information, or access to a candidate's social networking account, it does not prevent an employer from *requesting* either login information, or access to a candidate's social networking account. This presents some significant practical difficulties and inadequacies. Practically speaking, during the pre-employment process, if an employer requests access to a job candidate's social networking account (either by requesting the password or requesting the candidate login in the presence of the employer), the candidate is left with two choices. One choice the candidate has is to comply such a request. The other choice the candidate has is to refuse such a request. While under the Bill he or she legally has every right to make either choice, it is not out of the question to suggest that to choose the latter would likely cause the candidate to fall out of favour with the employer. A job candidate is in a very vulnerable position; the inequality in bargaining power referred to in Chapter 2 is very much at play in such a situation. A job candidate's 'consent' does not necessarily mean that he or she is fine with giving the

information or access to the employer; it could be nothing more than a product of the circumstance – the candidate wants the job. The request, while in the form of a request, is practically a condition in order to be given serious consideration. Furthermore, the provision in the Bill that prohibits an employer from penalizing any person because he or she has refused to comply with such a request clearly implies that the employer is entitled to make the request, such that it cannot be assumed, as a matter of interpretation, that a request is (because of a power imbalance) equivalent to an illegal demand. Moreover, this provision in the legislation is rendered practically ineffective for the same reasons (difficulty with proof) as human rights legislation (discussed above). In order for a candidate to have any reasonable possibility of success with a claim that the employer did not consider them because of their refusal to provide access to his or her social networking account, the employer would need to disclose that it was for this reason that they did not hire the candidate – practically speaking, even if this were the case, it is extremely unlikely that a mindful employer would do such a thing.

## **5.5 BRITISH COLUMBIA NDP INVESTIGATION**

In March 2011, The Office of the Information and Privacy Commissioner for British Columbia investigated the New Democratic Party of British Columbia's use of social networking and passwords to

evaluate potential candidates.<sup>189</sup> At issue was a practice by the BC NDP to ask candidates for passwords to their social networking content as a response to an incident from a previous provincial election after controversial photographs of an NDP candidate surfaced on Facebook.<sup>190</sup> The purpose of the investigation was to determine whether, under *BC PIPA*, the collection of the passwords was appropriate in the circumstances. Because candidates are not employees of the party, the information was deemed to be “personal information” as opposed to “personal employee information.” Nonetheless, the only real difference is that were it deemed personal employee information, the party would not need the consent of the candidate to collect the information and in this case because the party collected the passwords of the candidates, consent was obviously given. The standard for the collection of the information is that it can only be for purposes that a reasonable person would consider appropriate in the circumstances.<sup>191</sup>

To determine reasonableness, the investigation evaluated several factors: the purposes of collection and surrounding circumstances, the kind and amount of information collected, the uses to which it will be

---

<sup>189</sup> Summary of the Office of the Information and Privacy Commissioner’s Investigation of the BC NDP’s use of social media and passwords to evaluate candidates, P11-01-MS, online: <[http://www.oipc.bc.ca/Mediation\\_Cases/PDFs/2011.P11-01-MS.pdf](http://www.oipc.bc.ca/Mediation_Cases/PDFs/2011.P11-01-MS.pdf)> [*BC NDP Investigation*].

<sup>190</sup> *BC NDP Investigation*, *ibid* at p 1.

<sup>191</sup> *PIPA BC*, *supra* at note 102, s 11.

put, and whether the BC NDP had any reasonable alternatives to achieve its goals.<sup>192</sup> The investigation acknowledged that logging into an individual's social networking account gives the user access to an excess of information, and found that BC NDP collected a large amount of information, including information that may be outdated, irrelevant or inaccurate.<sup>193</sup> Furthermore, it found that BC NDP collected information about third parties that it did not have consent to collect.<sup>194</sup> Finally, it found that BC NDP did not explore any other reasonable alternatives.<sup>195</sup> As a result, the Privacy Commissioner found that the BC NDP did not have the authority to collect the passwords of candidates under *BC PIPA*.<sup>196</sup>

While this case does potentially provide some insight as to how similar cases might be treated in the employment context, it is important to note that the nature of choosing a political candidate to represent a political party is different from choosing an employee. More and more politicians and political candidates are using social networking in the capacity of their positions to connect with voters and constituents. Perhaps an analogy can be made between a political party looking into a candidate's social networking account and an employer

---

<sup>192</sup> *BC NDP Investigation, supra* at note 189 p 2.

<sup>193</sup> *BC NDP Investigation, ibid* at p 2.

<sup>194</sup> *BC NDP Investigation, ibid* at p 4.

<sup>195</sup> *BC NDP Investigation, ibid* at p 3.

<sup>196</sup> *BC NDP Investigation, ibid* at p 4.



looking into the account of a candidate who is being considered for a position in public relations or a related field. However, a key difference is that a political party is choosing the person to *be* their candidate – not a person to *fill a position* as a candidate. The links between the position and the candidate’s personhood are very strong in the political situation, and the public relations aspect of the position is absolutely paramount. In most employment situations, on the other hand, while it is important what kind of personal life the job candidate leads<sup>197</sup>, it is much less “reasonable” for an employer to feel a need to pry into the personal affairs of the job candidate. Nonetheless, here the NDP was seeking to perform the most intrusive of social networking background checks, and to do so was found to be a violation of *PIPA BC*.

## **5.6 FACEBOOK’S REACTION**

On March 23<sup>rd</sup>, 2012, Erin Egan, the Chief Privacy Officer of Facebook issued a statement titled “Protecting Your Passwords and Your Privacy.”<sup>198</sup> The statement condemns employers for requesting prospective employees to provide their passwords to their Facebook accounts. The statement warns employers that doing so could result in legal action from Facebook, warns users that to provide someone your password is a direct violation of Facebook’s Statement of Rights and

---

<sup>197</sup> To the extent that it is important if the employee is doing things in his or her personal life that affect the employment relationship.

<sup>198</sup> *Facebook Privacy Statement, supra* at note 34.

Responsibilities, and reiterates that every user has a right to keep their password to themselves. Finally, the statement asserts that Facebook will do everything in its power to ensure that this right is protected.

This has not amounted to all that much. Contrary to what was written, Facebook has not actually taken any legal action in this regard. In fact, even if Facebook did wish to do something, it is unlikely that they could take any action against an employer who has no relationship with Facebook.<sup>199</sup> What this essentially amounts to is Facebook giving notice to its users that it cares about their privacy – it could be seen as something of an advertisement. However, despite Facebook’s inaction, this statement does in some way display that Facebook is aware that its users are experiencing privacy concerns, and while Facebook may not be taking legal action for this type of violation of its Statement of Rights and Responsibilities, its actions (including its aforementioned compliance with the requests of the Office of the Privacy Commissioner) have shown a willingness to strive towards securing effective privacy controls for its users.

## **5.7 PRIVACY COMMISSIONER SOCIAL NETWORKING BACKGROUND**

### **CHECK GUIDELINES**

---

<sup>199</sup> A fundamental principle of contract law stipulates that only a party to a contract may sue on it (subject, of course to certain exceptions that would not apply here i.e. third party beneficiary rule) See Andela Swan, Jakub Adamski et al, “Contracts” *Halsbury’s Laws of Canada* (2012) online (QL) at HCO-64.

The Privacy Commissioners of both Alberta and British Columbia have released guidelines for employers with respect to statutory compliance specifically in the practice of conducting social networking background checks for prospective employees.<sup>200</sup>

The guidelines from the British Columbia Privacy Commissioner identify the following three possible risks that an employer could most likely encounter<sup>201</sup> when conducting a social networking background check: overreliance on an individual's consent to the collection of the information, the amount and relevancy of the information collected during the background check, and the accuracy of the information.<sup>202</sup> While these guidelines are useful in that they point out some of the potential dangers of social networking background checks to employers, they do not address or seem to solve any of the core problems that can result from a social networking background check.

In terms of information accuracy, the Guidelines point out that in any social networking background check, there is a risk that the information found could be inaccurate. For example, the Guidelines

---

<sup>200</sup> See Office of the Information and Privacy Commissioner for British Columbia, *Guidelines for Social Media Background Checks* (October 2011), online: <<http://www.opic.bc.ca/pdfs/private/guidelines-socialmediabackgroundchecks.pdf>> [*BC Guidelines*]; and Office of the Information and Privacy Commissioner of Alberta, *Guidelines for Social Media Background Checks* (December 2011), online: <[www.oipc.ab.ca/downloads/documentloader.ashx?id=2933](http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2933)> [*Alberta Guidelines*].

<sup>201</sup> In terms of violations of privacy legislation.

<sup>202</sup> *BC Guidelines, supra* at note 200.

specifically warn of mislabeled photos, out-of-date information, viewing the wrong profile altogether, or even viewing a profile that was set up by an imposter.<sup>203</sup> There is an obligation under all applicable Privacy legislation that the employer collects accurate information.<sup>204</sup> In conducting the social networking background check, employers open themselves up to a very real possibility of collecting inaccurate information, especially considering the fact that in British Columbia (or Alberta, for that matter) there is no requirement placed on the employer to first obtain the consent of the candidate to perform the social networking background check.

The problem here is that if the background check is being conducted by only the employer, and the candidate does not view and validate or invalidate the information, there is absolutely no way for the employer to know for certain whether the information is accurate. Furthermore, for information that the employer sees that is of such a nature that to take it into consideration would amount to discrimination in human rights law, the employer has a specific interest in not mentioning the information to the candidate, for fear of a human rights complaint if the candidate is not hired; this increases the likelihood of the collection of inaccurate information, because the candidate will

---

<sup>203</sup> *BC Guidelines, ibid* at p 2.

<sup>204</sup> See, for example, *PIPA BC, supra* at note 102, s 30.

likely not get the chance to validate or invalidate the information that is obtained.

In terms of overreliance on consent, the Guidelines warn employers to be mindful of who has given consent. While *BC PIPA*, for example, does not require consent for personal information about an individual that is collected, used, or disclosed for the purposes reasonably required to establish, manage, or terminate a contractual employment relationship, it does not allow for the collection of personal information of people who are not job candidates, or information that is not reasonably required for employment purposes (i.e. third party information). A social networking background check is almost certain to lead an employer to information about individuals other than the job candidate. As a result, the personal information about those third parties will certainly be viewed without that third party's consent, and the employer, as a result, would be running afoul of the legislation.<sup>205</sup> The problem with this is that the third party would need to be the one to launch a complaint with respect to the unauthorized collection of their personal information – and they are likely to be completely unaware that their personal information is actually collected. Furthermore, in terms of the consent of the candidate, as was discussed above in this Chapter, there are inherent issues as to whether the

---

<sup>205</sup> *BC Guidelines, supra* at note 200, page 3.

candidate's consent is tantamount to actual consent, or whether it is more so a product of their vulnerability in the situation (i.e. they are trying to get a job).

In terms of the collection of irrelevant information, the Guidelines merely warn of the superfluity of information that can be obtained via a social networking background check. Some of that information will likely not be permitted to be collected under almost all personal information privacy statutes (not to mention human rights statutes or even labour relations statutes).<sup>206</sup> While the warning is absolutely warranted, the fact that the social networking background check contains all of this information is likely exactly the reason why the employer wishes to perform the background check – it can contain all of this information and insight about the candidate. Employers already know this. If they did not know this, social networking background checks likely would not exist.

One reality that is missed here is that while viewing social networking information does amount to collection of personal information under privacy legislation, the actual process of navigating a social networking account is more akin to “viewing” than “collecting.” The hiring employer will view the account and the information contained therein. Regardless of whether they print the information

---

<sup>206</sup> *BC Guidelines, ibid* at p 3.

and collect it in some physical form, the information has been seen, and cannot be unseen. What is seen will, no doubt, factor in some way into the hiring decision – if it were not important, the social media background check would be forgone. But because of the non-physical, “viewing” nature of a social networking background check, significant issues are presented when it comes to any proof of misuse of the information. Both privacy and human rights legislation fail to address this reality, as they require some proof of a specific use or collection of particular information, and an employer merely viewing the information on their own does not generate any tangible proof.

The Guidelines provides suggestions for employers who still wish to perform social networking background checks but do not want to risk running afoul of privacy legislation. The suggestions are fairly straightforward and do not offer any real substantial advice beyond suggesting that employers be aware of their statutory obligations and be mindful to not try to circumvent them in a sneaky way. It is my belief that this is a product of the fact that absent demanding a password, or an honest admission from the employer of what exactly they saw and how it factored into the hiring decision (something no mindful employer would do), current privacy and human rights legislation are practically ineffective regulators of the pre-employment social networking background check process. They are not in tune with the actual practice

and nature of social networking background checks, they do not adequately take into account consent issues, their collection standard of “reasonableness” is insufficient in terms of direction, and, as a result, their practical impact is neither responsive to nor regulative of the problems this practice presents.



## **CHAPTER 6      Application of Current Law to the Employment Phase**

As is the case with the pre-employment phase, employers are increasingly incorporating the practice of creeping on the social networking activity of current employees. When examining social networking activity, it is possible for countless situations to occur that give rise to employment law issues. In examining the activity alone (without considering the different nature of social networking activity as opposed to activity in the physical world) first principles of employment law can be, and are, applied to address these situations. In Canadian employment law, an employee can only be terminated if there is just cause, or if the employee is given reasonable notice (or payment in lieu of that notice).<sup>207</sup> When it comes to application of first principles of employment law to dismissals as a result of social networking (or more general computer-use) activity, the question becomes whether the online activity of the employee constitutes just cause for dismissal or discipline. An examination of the current application of employment law to issues arising from social networking activity follows.

### **6.1 EMPLOYEE MONITORING IN THE WORKPLACE**

When an employee is at work, the employer has a vested interest

---

<sup>207</sup> Geoffrey England et al, “Employment” *Halsbury’s Laws of Canada* (2011 Reissue) online (QL) at HEM-301.

in the way in which the employee is spending his or her time. As such, it is important for an employer to be able to ascertain what an employee is doing during working hours. This right of an employer to monitor the at-work activities of an employee has been legally explored. The general rule is that employers do have a right to monitor the activity of employees; however, the real question is the extent and method the employer can use to monitor the activity of employees. At issue in one labour arbitration was the extent to which an employer could use video cameras to monitor employees while at work.<sup>208</sup> While the arbitrator in this case wrote that cameras present a technology to employers that allow them to be constantly supervising the activity of employees, the arbitrator also stressed that an employer's ability to use such technology must be balanced against the employees' legitimate interest in not being constantly surveilled; in assessing that balance, the arbitrator looked at the seriousness of the problem being addressed, the effectiveness of the cameras in addressing that problem, and the availability of other methods to address the problem.<sup>209</sup> In this case, the collective agreement gave management the right "to make, alter and enforce, from time to time, rules and regulations, policies and practices,

---

<sup>208</sup> *Re United Food and Commercial Workers Union, Local 1000A and Janes Family Foods (Surveillance Grievance)*, [2006] OLA No 611 (Trachuck) (QL) [*Surveillance Grievance*].

<sup>209</sup> *Surveillance Grievance*, *ibid* at paragraph 38.

to be observed by its employees.”<sup>210</sup> Taking this into account, the arbitrator found that the employer had a right to install cameras at strategic points (i.e. entrances and exits), but not at all places where the employees worked.

While there exist cameras that are so small they can go undetected, for the most part, if there is a camera watching your activity, you are aware of the camera’s presence. Certain other forms of monitoring can easily go undetected, and thus, can be implemented without any form of consent or knowledge on the part of the employee. In employment law, it has been found that to secretly audiotape what goes on in the workplace is improper; however, it was found that in order to correct this practice, the employer need only inform the employee that such audiotaping is occurring.<sup>211</sup> Similarly, under the *Criminal Code*<sup>212</sup>, a person is prohibited from using an electromagnetic, acoustic, mechanical, or other device to intercept a private communication (which is defined as communication made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the intended

---

<sup>210</sup> *Surveillance Grievance*, *ibid* at paragraph 26.

<sup>211</sup> *St Mary's Hospital v HEU*. (1997) 64 LAC (4th) 250 (BC) [Larson]. Here, the employees had agreed to the installation of certain surveillance devices for certain reasons. The employer alleged that this meant the employees acquiesced to being monitored in any number of ways. It was found that they did not.

<sup>212</sup> RSC 1985, c C-46, as amended [*Criminal Code*].

recipient<sup>213</sup>); however, as is the case in Employment Law principles, this does not apply where there exists express consent from the originator or recipient of the communication.<sup>214</sup>

## **6.2 MONITORING OF AT-WORK COMPUTER ACTIVITY**

With technology progressing the way it is and becoming more intertwined with our daily lives, employees are spending more and more time online (whether it be for work purposes, or for personal purposes). As a result, the issue of an employee giving his or her employer his or her full time and attention becomes more at issue than it has been in the past. In this context, what is meant by ‘full time and attention’ is that during an employee’s working hours, he or she will devote all of her attention and energy into the responsibilities for which he or she is employed, and avoid engaging in activities that are unrelated to work or wholly personal in nature<sup>215</sup>. For some jobs, social networking activity is part of an employee’s responsibilities; however, for most, it is not.<sup>216</sup> While this issue is not unique to social networking (it applies equally to general internet-surfing and phone use, for example), the personal nature and frequency of social networking use raises specific concerns to

---

<sup>213</sup> *Criminal Code, ibid* at s 183.

<sup>214</sup> *Criminal Code, ibid* at s 184.

<sup>215</sup> Obviously, employees do not devote absolutely *all* of their hours in the workplace doing work related tasks – people socialize in the workplace, take breaks, etc.

<sup>216</sup> For example, certain newspaper, radio, and television station employees incorporate social networking into their tasks as employees.

employers with regard to an employee's full time and attention. Excessive use of the Internet and social networking for personal web surfing has resulted in suspensions,<sup>217</sup> and even dismissals<sup>218</sup> of employees. Generally, however, excessive online activity has not been held to constitute time-theft. Time-theft is considered to arise when there is an element of fraud to the act (i.e. getting a co-worker to punch a time-card on your behalf).<sup>219</sup> While spending working hours surfing the internet or navigating Facebook for lengthy periods every day when it clearly is not a part of an employees job is, without a doubt, working-time spent doing something that is not part of the employment contract, the level of discipline that is considered appropriate for such activity seems to exist on a continuum, depending on the surrounding circumstances (e.g. content of the websites accessed, whether the employee had other things to do, frequency of the activity, etc.). The

---

<sup>217</sup> See *Health Sciences Association of British Columbia v Fraser Health Authority (Surrey Memorial Hospital)* [2011] BCCAAA No 125 (Glass) where a hospital employee who engaged in excessive Facebook and internet-use at work was given a 15-day suspension; and *FA v Deputy Head (Department of Citizenship and Immigration)* 2011 PSLRB 100 [*Andrews Grievance*] (Rogers) where a public service employee was given a lengthy two year unpaid suspension.

<sup>218</sup> See *Ontario Public Service Employees Union v Ontario (Ministry of Community and Social Services)* [2011] OGSBA No 167 (Johnson) where two employees were dismissed for using work computers to moderate a hurtful office blog, access hard-core pornography, and work on outside business ventures; and *DD v HA* [2008] BCHRTD No 361 where an employee who engaged in several hours of Facebook activity a day on the employer's work computer was forced to resign.

<sup>219</sup> *Andrews Grievance, supra* at note 217 at paragraph 78.

distinction here is that time-theft automatically leads to cause for dismissal, whereas excessive personal computer use does not necessarily.

As a result of all of this, once again, an issue becomes the manner and extent to which an employer can monitor an employee's computer activity. Screen Capturing and Keystroke Logging programs can be very effective in terms of monitoring an employee's activity on a computer. These programs do essentially what their name implies. Keystroke Logging programs capture all of the keystrokes made on a particular program and screen capturing programs take random or triggered photos capturing all that is visible on a certain computer screen. When there are keystroke logging or screen capturing programs installed on a computer or network of computers, unless the user is very computer savvy, there is no way of knowing that these programs are on the computer. As such, an employer can install these programs without an employee having any idea that the programs exist and issues surrounding employee awareness and consent can easily be practically circumvented via this technology. In this regard, a parallel can easily be drawn between monitoring an employee via audiotaping, and monitoring computer and social networking activity via computer program. In light of the employment and criminal law consent principles discussed above, many workplaces are now implementing

social networking policies, or general internet-use policies as a part of employment contracts. Sometimes these policies place a limitation on the extent to and purposes for which an employer can monitor computer use (i.e. virus protection, bandwidth monitoring, if there is reason to believe of a technical problem, troubleshooting, etc.), but it is possible for the policy to simply say that the employer either may or will monitor all activity that takes place on a work computer. This way, employees are given notice and consenting to the fact that the employer is monitoring his or her online activity, and gives proof to the employer that the employee has consented to such monitoring – employers are free to ‘keep calm and creep on.’

Is this appropriate? Not only is the validity of the consent in such a situation suspect, but while audiotaping and computer monitoring programs are similar in that they can go unnoticed (hence, a requirement of notice and consent), they are very different in terms of the potential content of what is being monitored. Audiotaping at work has a very real, spatial connection to the workplace – the conversations occur in the workplace. The computer, on the other hand, is different. While the computer is physically in the workplace, what happens on that computer in cyberspace does not necessarily have a content-related connection to work. Oddly, much of the case law and legal literature does not explore this. How exactly the employer came to find out about

the computer activity is rarely discussed. The focus, rather, is on the application of current employment law as to whether what is discovered through the monitoring justifies dismissal or suspension. A very important issue, the monitoring itself, is going unexamined.

### **6.3 EMPLOYER CONCERNS REGARDLESS OF LOCATION**

An employer's interest in an employee's activity is not limited to situations in which the activity in question occurs at the physical workplace. Given the lack of physical space to the cyber-world, certain employment law issues can arise from social networking and internet use regardless of the physical space in which the employee is acting. The general rule here (for all conduct, not only internet-use) is that in making employment-related decisions, an employer can only consider the conduct of an employee when he or she is off-duty if that conduct in some way relates to the individual's employment with that employer.<sup>220</sup> There are a few situations in which this is the case.

The first situation is when the conduct of an employee detrimentally affects the employer's reputation.<sup>221</sup> Given the instantaneous nature of social networking (and general internet) activity, and the potentially wide audience it can reach, reputations can be built and diminished in mere seconds. One way an employee has

---

<sup>220</sup> Access to Information and Privacy, *supra* at note 80, HAP-288.

<sup>221</sup> Access to Information and Privacy, *ibid* at HAP-288.



been found to detrimentally affect the employer's reputation is to make public comments that explicitly criticize the employer.<sup>222</sup> In the social networking context, if someone were to write a Facebook status to the effect of "What a terrible day at work. I absolutely hate my employer and think he might be the most unfair, rude, and inconsiderate person I have ever had the displeasure of meeting. It would bring joy to my heart if he dropped dead," his or her employer, as a human being or business, has a legitimate interest in knowing that such comments were made, and if the employer found out the statement was made (for example, if the employer and the employee were Facebook friends) it is entirely possible that the employee could be fired for cause (i.e. insubordination).<sup>223</sup> This very thing happened in *Lougheed Imports Ltd. (West Coast Mazda) v. United Food and Commercial Workers International Union, Local 1518*;<sup>224</sup> two employees were discharged for posting very disrespectful, insulting, and offensive comments about their supervisors and managers on Facebook.

However, not only comments directed at an employer can damage the reputation of the employer. Whether an employer interest exists on

---

<sup>222</sup> See *Re Inco Metals Co and United Steelworkers*, [1978] OLAA No 2, 18 LAC (2d) 420 (Weatherill), and *Re United Auto Workers, Local 444 and Chrysler Corp of Canada*, [1961] OLAA No 1, 11 LAC 152 (Bennett).

<sup>223</sup> The way that an employer should be able to go about discovering whether such a statement was made will be explored in greater detail in Chapter 8.

<sup>224</sup> 2010 CanLII 624482 (BCLRB).

this basis is determined by considering whether the employer's reputation is clearly damaged by the off-duty actions of an employee considering all of the surrounding circumstances.<sup>225</sup> In making this connection, it is insufficient to show that the employer is well-known with an image to protect – the employee's off-duty conduct must implicate the employer in some way and has to be such that continuing to employ the employee would sully the employer's reputation.<sup>226</sup> Also adding to the surrounding circumstances are factors relevant to the employee, like, for example, the position that the employee holds within the employer's company.

This can certainly occur online. In *EV Logistics v. Retail Wholesale Union, Local 580 (Discharge Grievance)*,<sup>227</sup> for example, an employee identified his employer on his blog, but did not criticize that employer. The subject matter of the blog, however, was the problem. On the blog, the employee posted many racist remarks and expressed adoration for Adolph Hitler and the Nazi Regime. While the arbitrator noted that the blog was not directly aimed at the employer and found that termination was too severe a punishment, it was decided that because the blog mentioned the employer coupled with the nature of the

---

<sup>225</sup> *Re Ford Motor Co of Canada Ltd. and UAW, Local 200* (1964), 15 LAC 349n (Lang).

<sup>226</sup> *Re Madame Vanier Children's Services and Ontario Public Service Employees' Union*, [1988] OLA No 2, 5 LAC (4th) 225 (Verity).

<sup>227</sup> [2008] BCCA No 22 (Laing).

content of the blog, the employer had a right to discipline the employee regardless of the fact that the activity took place outside work.

Another situation in which off-duty conduct can relate to an individual's employment is if the conduct adversely affects the employee's ability to discharge his or her duties and responsibilities.<sup>228</sup> Consider, for example, an employee working in the health care sector. One of the duties of many employees working in the health care sector is to keep certain information confidential. In such a situation, the employer has an interest in ensuring that the employee does not violate his or her obligation to keep that information confidential, because if that employee discloses confidential information to others, it is a violation of his or her duties and responsibilities regardless of the physical location in which such disclosure took place. This type of violation can very easily occur online. In one case,<sup>229</sup> the employee, a personal care giver at a nursing home, set up a blog where she published text, pictures and comments about various residents of the nursing home without their consent. While the blog was written on the employee's own time, the employee argued that the comments made were akin to what employees normally discuss during break times and

---

<sup>228</sup> Access to Information and Privacy, *supra* at note 80, HAP-288.

<sup>229</sup> *Chatham-Kent (Municipality) v. National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada), Local 127* (Clarke Grievance), 159 LAC (4th) 321, [2007] OLAA No 135 (Williamson) (QL).

was not out of the ordinary; however, the arbitrator, pointing to the fact that the employee had signed a confidentiality agreement and that the blog was accessible to anyone with an internet connection, rejected that argument and ruled that the employee's termination be upheld – the employee's online conduct was in violation of her and the employer's duty of confidentiality.

The final situation in which an employee's off-duty conduct has been found to affect his or her employment is if the conduct affects the employment rights of other employees.<sup>230</sup> Something that fits squarely within this category is harassment among coworkers. Employers also have a statutory interest in monitoring this type of activity. Under the *Ontario Human Rights Code*,<sup>231</sup> employers have a obligation to respond to discrimination or harassment in relation to a prohibited ground, and under Ontario's *Occupational Health and Safety Act*,<sup>232</sup> employers are required to address workplace violence and harassment by proactively implementing policies, training programs, and identifying problem employees.

With social networking, conversations that were once held privately around the water-cooler are now spread online<sup>233</sup>, adding

---

<sup>230</sup> Access to Information and Privacy, *supra* at note 80, HAP-288.

<sup>231</sup> R.S.O. c. H.19 (1990)

<sup>232</sup> R.S.O. 1990, CHAPTER O.1, PART III.0.1

<sup>233</sup> See Robert Todd, "Facebook is the New Water Cooler: B.C. Ruling Shows Venting on Online Social Media Sites Can Lead to Getting

elements of physical disconnect between the parties and instantaneity in the dissemination of gossip. As a result, employers have a legitimate interest in knowing when this type of activity is happening among co-workers, regardless of the fact that it is taking place online, rather than in the physical workplace.

*Alberta Distillers Ltd. v. United Food and Commercial Workers, Local 1118*<sup>234</sup> illustrates how workplace harassment can occur online. In this case, one employee (Conrad) complained to the employer that she had been the victim of malicious comments by another employee (Carlson) on a third employee's (Whiteside) Facebook wall. As a result, the employer investigated the matter and decided, in light of his obligation to provide a harassment-free workplace, to terminate Whiteside. However, there is a revealing wrinkle in this case. The malicious posts, while they existed on Whiteside's Facebook wall, were written by Carlson – Whiteside had not commented on the post or displayed any approval of the content of the wall post beyond not deleting the post. As a result, it was ordered that there was no cause for discipline, and that Whiteside be reinstated with backpay. However, what this shows is that not only can workplace harassment issues and subsequent terminations arise as a result of social networking activity, but also that confusion can ensue and wrong decisions can easily be

---

Fired”, *Canadian Lawyer Magazine* (February 2011) 39, 41.

<sup>234</sup> [2009] AGAA No 46.

made when an issue does arise via social networking activity, and the decision-maker does not fully understand how exactly social networking operates.

Indeed, as can be seen from all of the aforementioned examples, there are numerous reasons, legal and otherwise, for an employer to concern himself or herself with what an employee is doing on social networking sites even when that activity takes place during non-working hours. This is a given – this is acknowledged. However, this is not what I consider to be the real issue when it comes to social networking activity and its effects on the workplace. The real issue here is whether, and to what extent, does the employer have a right to access and monitor the employee’s social networking activity. Or, put another way, what kind of privacy right should the law afford an employee when it comes to keeping his or her social networking content away from the creeping eyes of his or her employer?

One decision that explored this very issue<sup>235</sup> was a privacy complaint in Alberta. In this case, the Calgary Police Service (a public body) was monitoring an employee’s work email activity as a result of a complaint from coworkers including allegations of inappropriate sexual

---

<sup>235</sup> Actually, it was not concerning social networking activity specifically, but the basic principles should still be applicable.

conduct.<sup>236</sup> At issue was not really whether the public body's monitoring of the employee's work email was permissible under the circumstances; what was at issue was the public body's use of something that was found in the email. In the employee's work email, there was a message that indicated the login information and password for the employee's personal email.<sup>237</sup> The employer used this information to access the employee's personal email and therein found photographs of a sexual nature that appeared to have been taken at the workplace; these photos were used in the public body's decision to terminate the employee, and were also used in the subsequent grievance process.<sup>238</sup> The employee made a complaint to the Privacy Commissioner that the use of this information was in contravention of Alberta's *Freedom of Information and Protection of Privacy Act*.<sup>239</sup> The adjudicator found that the collection of the personal information from the work email were not a violation of the *Act*, but the use of the login information and password (which led to the collection of the pictures) was in violation the *Act*, as logging into the employee's personal email account was exceptionally invasive, and not necessary for the public body to carry on

---

<sup>236</sup> Alberta Office of the Information and Privacy Commissioner, *Order F2012-07* – Calgary Police Service (20 April 2012) online: <<http://www.oipc.ab.ca/downloads/documentloader.ashx?id=3050>> [*Police Grievance*].

<sup>237</sup> *Police Grievance, ibid*, at paragraph 3.

<sup>238</sup> *Police Grievance, ibid*, at paragraph 3.

<sup>239</sup> *FIPPA AB, supra* at note 79.

its purposes in a reasonable manner (as is required under the *Act*).<sup>240</sup>

While this appears to suggest that employers cannot access the personal email password and inbox of an employee, there are a few particularities about this case that should be noted. First, in her decision, the adjudicator suggests that had the employee been accessing the personal email address at work, the result may have been different.<sup>241</sup> Second, as the employer in this case was a public body, the relevant legislation was Alberta's *FOIPA*, rather than *PIPA*. As discussed in Chapter 4, the standards for collection of personal information are much more stringent in the public sector than the private sector, especially for information that is classified as "personal employee information," as the information in this case would have been. Even worse, had this employee been working in a provincially regulated industry in one of the jurisdictions with no applicable privacy legislation, the employee's personal information would have had no statutory privacy protection whatsoever (besides the tort of "intrusion upon seclusion"). Finally, it is important to note that the employer was attempting to use the information collected in an official capacity – the employer was trying to use the photographs obtained as grounds for termination of the employee. This puts the photographs under direct

---

<sup>240</sup> *Police Grievance*, *supra* at note 236, paragraphs 29-30, citing *AB FOIPA* s. 39.

<sup>241</sup> *Police Grievance*, *ibid*, at paragraph 29.



scrutiny of the legislation, whereas if the employer had simply noted that the photographs existed and proceeded to treat that employee accordingly (i.e. waited for another reason for termination, not promoted as a result, etc.), the collection and use of these photographs would not have been under the scrutiny of the Act.

Beyond this case, the vast majority of the case law and legal literature concerning social networking activity during the employment relationship is much different from that with respect to the pre-employment phase. As was seen with the pre-employment phase, the big issue was the extent to which an employer could access a candidate's social networking activity – this is not-so-much the case with legal issues arising out of social networking activity of someone who at the time of the activity is under an employment contract with a specific employer. For example, in one case, a postal clerk with 31 years of service was dismissed as a result of certain insubordinate postings on her Facebook account.<sup>242</sup> The supervisor in this case was informed by another letter carrier that some employees were spreading rumours and writing inappropriate things about supervisors on Facebook.<sup>243</sup> The supervisor logged into Facebook under the account of a friend to protect his identity (something that is directly against Facebook's user agreement), and searched for employees who he felt were the

---

<sup>242</sup> *Canada Post Grievance*, *supra* at note 35.

<sup>243</sup> *Canada Post Grievance*, *ibid* at paragraph 30.

“disruptive” employees (i.e. the ones who he thought would be likely to write such things).<sup>244</sup> In doing so, he found the postings at issue in this case. However, the activity of the supervisor (logging into someone else’s account and accessing the employee’s Facebook page) was only mentioned in passing. The issues discussed and analyzed in the case were the contents of the postings, and whether they constituted grounds for dismissal – not whether it was appropriate for the supervisor to access the employer’s social networking information the way he did. While the supervisor was not himself breaching any of Facebook’s regulations, the way in which he accessed the posts does raise some concerns that I think should have been addressed. Unfortunately, the only real issue explored in cases and legal literature with respect to social networking activity in the workplace is the determination of whether the employee’s activity is cause for dismissal or discipline, and not whether the employer should be able to monitor the social networking activity of the employee at all.

There is something strange about all of this. At the pre-employment phase, employers seem to come off as aggressively pursuing a candidate’s social networking information. There are media reports of employers asking for a candidate’s Facebook login information, warnings from Privacy Commissioner’s Offices about such

---

<sup>244</sup> *Canada Post Grievance*, *ibid* at paragraph 30.

activity, and legal blog posts exploring the legality of these types of practices. However, once the employment relationship is established, employers do not seem to be so aggressive – with the exception of the Calgary Police case mentioned above, there are very few cases where the employer seems to be snooping into an employee’s personal online information. Between the time where an individual was a candidate and where that individual becomes an employee, something significant seems to have changed with respect to the employer’s overt interest in the person’s social networking activity. Why?

It could be that the employer’s approach is to be very thorough in its social networking exploration during the hiring process, and then trust that the right decision was made so much that he or she no longer has any interest in monitoring the employee’s social networking activity. While this is possible, and could be the case for some employers, it seems a bit simple to think that this is the approach taken by most employers. If the employer is interested in a potential employee’s social networking activity before the employment phase commences, given the plethora of situations in which an employer has an interest in an employee’s social networking activity discussed above, it seems only logical that that employer would be just as, if not more interested in the employee’s social networking activity once the employment relationship commences.

I contend that employers are still as interested, if not more interested in an employee's social networking activity as they are at the pre-employment phase; however, the dynamics of the situation allow employers to creep the employee's activity with more secrecy. During the pre-employment phase, in order for an employer to access a candidate's social networking information, their only practical way of doing so is to ask the candidate directly for said access (either by asking for login information, asking to become the candidate's "friend," or asking that the candidate login to a computer so the employer can browse the candidate's social networking account). Certain candidates have complained of this practice and there has been resulting legal response (legal blogs, Privacy Commissioner Guidelines and Human Rights Commissioner statements). Once the candidate becomes an employee, however, the way an employer can access social networking information changes. Employers have the ability to use technology to monitor the employee's online activity. As previously mentioned, through Keystroke Logging and Screen Capturing programs, an employer is able to monitor what an employee does on the computer without being detected. Or in a less invasive manner, an employer can even look through an employee's work email or web-browsing history without the use of any special program. The lack of overtness to this type of monitoring explains why there have been few complaints about

such monitoring during the employment relationship – employees do not necessarily know it is happening. Furthermore, the lack of employment standards protection afforded to candidates at the pre-employment phase provides further insight into this discrepancy. If an employer, as a result of looking at a candidate’s social networking activity decides that he or she does not want to hire the candidate, the employer can simply state that they felt someone else was a better fit, or some other reason to explain their hiring decision (whether it is true or not). Employers are not under any real obligation to be honest, or cite an objectively valid, legislated reason for choosing to not hire someone. During the employment phase, if an employer wishes to terminate someone, the employer needs to show that there is just cause for doing so, or give reasonable notice (or payment in lieu of notice). As a result, if an employer creeps an employee’s social networking activity and finds something distasteful, the employer is not permitted to terminate the employee as a result of what he or she has found unless the findings are sufficient cause for dismissal. This explains why the cases emerging involving an employer monitoring an employee’s social networking activity are primarily those where the real analysis is whether the conduct justifies dismissal or discipline – it is only situations in which the employer is using the social networking activity in an official capacity to justify terminations or discipline. In practical reality,

employers can easily monitor the online activity of his or her employees, take mental note of the activity, and proceed to treat the employee accordingly using what was seen in an unofficial capacity (i.e. not really consider them for a promotion, wait for any other excuse for discipline or termination, etc.).

As a result of all of the factors mentioned in the paragraph above, it is my belief that the small number of cases where an employer is known to have monitored social networking of current employees is probably not representative of the extent of creeping that is actually going on. Consequently, the fact that there is such a small number of cases where an employer is known to be monitoring the social networking of current employees seems to contribute to the lack of recognition of the the seriousness of the privacy issues at stake when such creeping occurs.

When it comes to privacy legislation, the exact same problems that exist during the pre-employment phase exist during the employment phase. Even if the employee gives consent for his or her employer to view his or her social networking activity, there are issues as to whether that consent is reliable or merely a product of the bargaining power of the two parties; furthermore, third-party consent and the resulting privacy problems is still a major issue that is essentially impossible to be addressed under the current legislation.

The collection standard of what is ‘reasonable’ is very vague, and without voluntary disclosure from the employer of what was ‘collected,’ the practical nature of viewing online activity is more akin to viewing than collecting, as an employer needs only see the information to make unofficial use of it, rather than printing the information and physically collecting it. And finally, when it comes to information contained on social networking sites, there are major questions surrounding accuracy and reliability of the information.

What this all amounts to is that there are many problems when it comes to protecting an individual’s privacy interest in his or her social networking information. It is my position that this is because we are conceptualizing the way in which we protect social networking information incorrectly. As a result of this misconceptualization, the mechanisms we employ to actually protect the information is fraught with holes and deficiencies. In Chapter 7, I will explain New Virtualism, which I believe offers insight into how we should conceptualize the protection of social networking information. It is my position that once this conceptualization is accepted, the degree to and way in which we protect social networking information becomes fairly straightforward.

## CHAPTER 7      New Virtualism Explained

One approach to the regulation of online activity is to simply apply the law of the physical world to the online world without much consideration of the different nature of the two spaces. This appears to be what is happening in the context of employment law issues when it comes to the use of social networking – first generation employment law principles are applied to situations without any real contemplation of the idea that there is a different nature to activity that takes place in the online world than activity that takes place in the physical world. When it comes to privacy, the law views the information generated by an individual’s online activity as a kind of physical “thing” in which the individual, by virtue of his or her connection to that thing, has some sort of property interest. This is what is referred to as an “externalist” approach, and it will be discussed in more detail later in this Chapter. For now, I want to say that I do not think an externalist approach is adequate or appropriate. I believe that an emerging body of scholarship called “New Virtualism” provides a sounder theoretical basis upon which legal issues arising from social networking use should be based. Drawing upon certain core principles of past Virtualist<sup>245</sup> theories that

---

<sup>245</sup> Early scholars who wrote of cyberspace as a separate world have been dubbed “Virtualists” by James Grimmelman in “Virtual Borders: The Interdependence of Real and Virtual Worlds” *First Monday* (6 February 2006) online:



did not work out, New Virtualism finds a balance between certain aspects of early cyberlaw theories and new practical legal realities with respect to the way in which contemporary internet use is affecting the way we live in the physical world. An exploration of the origins of New Virtualism, as well as its virtues, follows.

The first generation of cyberlaw scholarship, Virtualism, came about when the internet was still young and not used nearly to the extent to which it is today. The foundational idea behind Virtualism was the “Uniqueness Thesis”. The Uniqueness Thesis acknowledged that the online world was a completely new and unique place that was of a much different nature than the physical world.<sup>246</sup> The physical world and the online world were conceived of as being two completely distinct spaces, with clear-cut territorial borders.<sup>247</sup> From this idea emerged the belief that because of its different territorial space and lack of physicality, the ‘space’ that is the online world should, and would be free from any external governmental control of influence – it dismissed real space concerns from the conversation when it came to

---

<[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=868824](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=868824)> [*The Interdependence of Real and Virtual Worlds*].

<sup>246</sup> Jonathon Penney, “Understanding the New Virtualist Paradigm” (2009) *Journal of Internet Law* 12 at 2 [*Understanding the New Virtualist Paradigm*].

<sup>247</sup> David R Johnson and David Post, “Law and Borders: The Rise of Law in Cyberspace” (1996) 48 *Standord Law Review* 1367 [*Law and Borders*].

cyberspace.<sup>248</sup> This is what was known as the “Legal Immunity Thesis”. John Perry Barlow’s *A Declaration of the Independence of Cyberspace* is a clear example of the way in which early cyberspace scholars shunned the idea of legal regulation of the virtual world.<sup>249</sup> However, when Barlow’s *Declaration* was written, the internet was in its infancy and used in a way that had little to no direct impact on the physical world. Since then, the way in which the internet is used has changed drastically. We need only look at the fact that real-money trade occurs online to demonstrate that the borders are not-so distinct; commercial transactions that occur online have corresponding real-world elements, obligations, and regulations.<sup>250</sup> As a result of this changing nature of the use of the internet, it became vulnerable to traditional forms of control from physical world forces. There is most definitely government regulation and lawmaking with respect to that which goes on in the online world – it is far from immune to outside influence. It is now apparent that the hopes and visions of those who advocated for online legal immunity did not work out.

---

<sup>248</sup> Understanding the New Virtualist Paradigm, *supra* at note 246, 2-3; See also Orin S Kerr, “Enforcing Law Online” (2007) 74 U Chi L Rev 745, 745, 751.

<sup>249</sup> Written February 8, 1996. Available online at <<https://projects.eff.org/~barlow/Declaration-Final.html>> [*Declaration*].

<sup>250</sup> *The Interdependence of Real and Virtual Worlds*, *supra* at note 245, 7.

New Virtualism, while acknowledging that the original Virtualists were incorrect about the online world's legal immunity, contend that there are still lessons to be learned from the original Virtualists, as "the Virtualist intellectual paradigm was never really about law or politics, at least not directly. Rather, it was about the fundamental nature of cyberspaces and virtual worlds themselves."<sup>251</sup> New Virtualism contends that just because the Legal Immunity Theory was incorrect does not mean that the Uniqueness Thesis upon which the Virtualists based the Legal Immunity Thesis cannot provide a solid foundation upon which approaches to legal regulation of online activity should be based.<sup>252</sup> It is for this reason that the theory is called "New" Virtualism – it embraces the Virtualist idea that the uniqueness of cyberspace poses challenges to law and policy that need to be approached differently than real space challenges; however, it is "New" in the sense that it goes beyond the utopian ideas of the Legal Immunity Thesis, and approaches the challenges posed to real space and cyberspace together, acknowledging the importance, coexistence, and interdependence of the two worlds.<sup>253</sup>

What innovations does this new theory offer? In the article *Understanding the New Virtualist Paradigm*, Jonathon Penney writes

---

<sup>251</sup> *Understanding the New Virtualist Paradigm*, *supra* at note 245, 2.

<sup>252</sup> *Understanding the New Virtualist Paradigm*, *ibid* at 2.

<sup>253</sup> *Understanding the New Virtualist Paradigm*, *ibid* at 2-3.

that “the best way to understand the New Virtualism is to compare it with the intellectual product of the first generation cyberlaw scholars – the original Virtualists.”<sup>254</sup> In doing so, Penney sets out the following three key features or innovations that are found in New Virtualism theory that were not a part of the original Virtualist theory – innovations that are more responsive to and appropriate for the way in which the internet is being used in contemporary society: “first, its recognition of the permeability of real and virtual space; second, its reliance on the interdependence of cyberlaw analytical perspective; and third, its rejection of the cyber-utopians Legal Immunity Thesis.”<sup>255</sup>

## **7.1 THE PERMEABILITY OF REAL AND PERSONAL SPACES**

Original Virtualists were of the opinion that cyberspace was defined by clearly marked boundaries that made it physically separate from real space.<sup>256</sup> Virtualists believed that these borders between real space and cyberspace (in the forms of screens and passwords) were hard, clear, and defined – they created territorial boundaries that completely separated the two worlds.<sup>257</sup> As a result, the idea that real world laws and norms would apply to the cyber world was not

---

<sup>254</sup> *Understanding the New Virtualist Paradigm, ibid* at 3.

<sup>255</sup> *Understanding the New Virtualist Paradigm, ibid* at Abstract.

<sup>256</sup> See *Law and Borders, supra* at note 247.

<sup>257</sup> *Law and Borders, ibid* at 1367.

conceivable to the original Virtualists – the two spaces were thought to be impermeable.<sup>258</sup>

Over time, however, as a result of the changing nature of the way in which people use the internet, the original Virtualists idea of a clear border turned out to be wrong.

“...borders between real space and cyberspace were neither clear nor impermeable. Increasing public use and popularity of the Internet and its cyberspaces and virtual worlds, brought more attention and scrutiny from ‘real space’ state regulators and law enforcement officials. New laws were proposed and new means of controlling this supposed ‘new frontier’ of cyberspace were propagated and enforced, reaching into the presumably impenetrable borders of cyberspace. Increasing electronic commerce and commodification also played a role in blurring borders between cyber and real space. As business moved more of their commerce online, they sought new ways to track and influence consumer habits and preferences; that is, they brought traditional business ideas into the cyber world. The hard and clear borders of cyberspace were not so, and the cyberlaw proposals of the original Virtualists, based on this false assumption, were cast into doubt with these important changes.”<sup>259</sup>

New Virtualism, unlike the original Virtualism, acknowledges and embraces these uncertain borders between the physical world and the online world.<sup>260</sup> In doing so, New Virtualists do not need to ignore the fact that the goings on in the online world and the goings on in the real world are interrelated and interdependent; as a result, New Virtualists are in a better position than Virtualists to understand what effect

---

<sup>258</sup> *Law and Borders, ibid* at 1402.

<sup>259</sup> *Understanding the New Virtualist Paradigm, supra* at note 245, 4.

<sup>260</sup> *Understanding the New Virtualist Paradigm, ibid* at 4.

traditional laws should and will have on the norms of virtual spaces, and vice-versa.<sup>261</sup> This acknowledgement is altogether different from that of the original Virtualists. It does not conceive of the cyber world as being a clear-cut space, completely removed from the physical world – this is a crucial difference between the way in which Virtualism and New Virtualism conceive of the proper regulation of activity that occurs online. New Virtualism is more in tune with contemporary internet use.

## **7.2 RECOGNIZING THE IMPORTANCE AND INTERDEPENDENCE OF PERSPECTIVE**

The problem of perspective in approaching the legal regulation of online activity has been described as a conflict between “internal” and “external” viewpoints.<sup>262</sup> New Virtualism’s understanding of the borders between cyberspace and real space as not being clearly defined, but rather as interrelated and interdependent gives New Virtualism a perspective for analysis that was missing in the original Virtualist

---

<sup>261</sup> *Understanding the New Virtualist Paradigm, ibid* at 4-5.

<sup>262</sup> Orin Kerr, “The Problem of Perspective in Internet Law” (2003) 91 *Geo LJ* 357 at 357-405 [*The Problem of Perspective in Internet Law*].

theory of online regulation and allows for a more appropriate analysis that cannot be done from a wholly externalist perspective.<sup>263</sup>

Internal perspectives analyze something from the perspective of a ‘person’ who is living within a cyberspace or virtual community.<sup>264</sup> As can be seen in Barlow’s *Declaration*, the original Virtualists, because they saw the online world as a clearly defined space with territorial boundaries, embraced an internal perspective when it came to the regulation of online activity.<sup>265</sup> The external perspective, as previously mentioned, advocates for the use of the laws and regulations of the physical world, and merely applying them to the online world as if it exists in the physical world.<sup>266</sup> The external perspective was not used in any way by original Virtualists; it was seen as being appropriate for that “other place” (the physical world) that was completely removed and distinct from the cyber world – consequently, its norms and rules were considered inappropriate.<sup>267</sup>

The reality is that virtual people are in a very real way associated with real people, and virtual communities are designed by people who live in the physical world.<sup>268</sup> While this was not the case during the

---

<sup>263</sup> *Understanding the New Virtualist Paradigm*, *supra* at note 245, 7.

<sup>264</sup> *The Problem of Perspective in Internet Law*, *supra* at note 262, 357.

<sup>265</sup> *Declaration*, *supra* at note 249.

<sup>266</sup> *The Problem of Perspective in Internet Law*, *supra* at note 262, 357.

<sup>267</sup> See *Law and Borders*, *supra* at note 247 and *Understanding the New Virtualist Paradigm*, *supra* at note 245, 7.

<sup>268</sup> *Understanding the New Virtualist Paradigm*, *ibid* at 7.

Virtualist era, it is now the reality. As a result, New Virtualism values a balance between the internalist and the externalist perspectives. New Virtualist scholarship remains Virtualist in the sense that it understands the value that an internalist perspective can offer, but it also understands that an external perspective, as it can provide important insight, is not to be ignored.<sup>269</sup> According to New Virtualism, both the internal and external perspectives, the virtual and physical, are now relevant, necessary, and interrelated; as a result, it is more practical, applicable to the present state of internet use, and more flexible than a wholly internalist or wholly externalist perspective alone.<sup>270</sup>

### **7.3 REJECTING THE LEGAL IMMUNITY THESIS**

Flowing naturally from the premises discussed earlier – the permeability of the borders of real and virtual space – it is clear that New Virtualism cannot accept a perspective that is wholly internalist.<sup>271</sup> However, the rejection of the assertion that external laws should play no part in the virtual world does not mean that the internalist perspective is dismissed. While the recognition of interrelated boundaries implicitly rejects the Legal Immunity Thesis, it “also rejects the thesis of cyberlaw skeptics who see nothing interesting, unique, or

---

<sup>269</sup> *Understanding the New Virtualist Paradigm, ibid* at 7.

<sup>270</sup> *Understanding the New Virtualist Paradigm, ibid* at 8.

<sup>271</sup> *Understanding the New Virtualist Paradigm, ibid* at 8-9.



new [about the regulation of online activity], or that [the cyber world] is non-existent.”<sup>272</sup> Taking real life concerns into account is an acknowledgement that the same people live in the real world and in the virtual world, but it is not an abandoning of the idea that online activity should not be thought of differently than activity in the physical world; it is simply a recognition of the practical reality that the online world and the physical world are interdependent.<sup>273</sup> The end result is that New Virtualism calls for laws that are both sensitive to the unique nature of the virtual world, and cognizant of the fact that the virtual world is not a completely separate world that exists in complete isolation from the physical world; the original Virtualists were wrong to completely reject externalism, but to ignore the values of an internalist perspective would be just as misguided when it comes to making sound choices in policy and law when it comes to the regulation of activity that takes place in the online world.

#### **7.4 PRIVACY IN NEW VIRTUALISM**

As mentioned in Chapter 2, privacy is difficult to conceptualize. It has been said that the concept of privacy is in disarray, as it appears to be about everything, and therefore, about nothing.<sup>274</sup> As can be seen

---

<sup>272</sup> *Understanding the New Virtualist Paradigm*, *ibid* at 9.

<sup>273</sup> *Understanding the New Virtualist Paradigm*, *ibid* at 9.

<sup>274</sup> Daniel J Solove, “A Taxonomy of Privacy” (2006) 154 U Pa L Rev 477 at 477.

in Chapters 5 and 6, the advancement of technology and the changing nature of the use of technology presents new difficulties to an individual's privacy interests and, more generally, to conceptualizing what exactly privacy protects.

## **7.5 INFORMATIONAL PRIVACY: A PROBLEM**

The subject matter of privacy concerns with respect to online activity and personal information found online has generally been classified as “informational privacy.”<sup>275</sup> While it is difficult to conceptualize what exactly is meant by informational privacy, the Supreme Court of Canada has defined informational privacy, as opposed to personal privacy or territorial privacy as follows: “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”<sup>276</sup> Most legal scholars have approached informational privacy as a form of property interest, in that people should be able to control their online personal information because they have a property right in that information.<sup>277</sup> As was mentioned in Chapter 4, this was the type of privacy interest Justice Sharpe said was at stake in *Jones v Tsige*.

---

<sup>275</sup> *Virtual Communities and the Social Dimension of Privacy supra* at note 21 at paragraphs 24-25.

<sup>276</sup> *Tessling, supra* at note 23, paragraph 23 citing Alan F Westin, *Privacy and Freedom* (New York: Atheneum 1970) at 445.

<sup>277</sup> Jonathon Penney “Privacy and the New Virtualism” (2008) 10 *Yale J L & Tech* 194 at 206 [*Privacy and the New Virtualism*].

According to New Virtualist principles, this categorization of “informational privacy,” as a form of property is misguided. The categorization of privacy renders the conceptualization of privacy even more convoluted than it already is.<sup>278</sup> Not only this, but to view someone’s online information as property is looking at online activity from a wholly externalist point of view. In real space, when thinking of physical documents in a person’s possession it makes sense to distinguish between an individual’s right in privacy to make decisions and determinations with respect to his or her physical person and a person’s more so property-related right to determine whether to disclose the information contained in those physical documents as he or she pleases. The former has to do with decision-making for the self, whereas the second is more so about controlling a “thing” that contains information about the person. To think of someone’s online information as a “thing” over which they have proprietary control with respect to the disclosure or non-disclosure of that information is to think about the information as being the product of a real person sitting at his or her keyboard in physical space, external to the virtual space. But if one is to think of online information from an internalist perspective, if we think of the person as if they are choosing, moving, and negotiating within the virtual space, the distinction between a property interest in

---

<sup>278</sup> *Privacy and the New Virtualism, ibid* at 207.

information and the right to make decisions for the self blurs – in the online space, the information is what makes up the person.<sup>279</sup> As was written in Chapter 2, privacy is important because it allows people the ‘space’ necessary to achieve their personhood. As a result, rather than theorizing about under which categorization of privacy online information should be classified, New Virtualism asserts that in order to have a more appropriate understanding of what type of privacy protection online information should be given, it is more important to fully understand the nature of personhood in cyberspace.

## **7.6 PERSONHOOD IN CYBERSPACE**

In real space, a person’s body is easily defined through physical limits, and that together the “information” inside that person’s body (i.e. experiences, thoughts, morals, etc.) make up the individual. This “information” that is inside the person is not protected via “informational” privacy protection, it is protected and respected because it is viewed as being constitutive of an individual’s personhood. Unlike in real space, where a person’s body is discerned and defined through the physically fixed limits, the virtual person is embodied through information; the information is not the property of the person – the information is the person.<sup>280</sup> Online information is not a “thing;” rather,

---

<sup>279</sup> *Privacy and the New Virtualism, ibid* at 214.

<sup>280</sup> *Privacy and the New Virtualism, ibid* at 218-219.

“digital technology enables the preservation of the minutia of our everyday comings and goings, of our likes and dislikes, of who we are and what we own...a life captured in records, a digital person...”<sup>281</sup>

“Our identities, personal preferences, interests, relationships (online and offline), health, hobbies, and work are embodied in the information volunteered by us online, or collected about us through our daily sojourns in virtual worlds [and] electronic landscapes.”<sup>282</sup> What is put onto social networking sites, according to New Virtualism, is not just information, but rather a capturing of certain elements of our selves – the information makes up a virtual person. This is not to say that the virtual self is completely cut off from the physical self; rather, the two are intimately linked – the virtual person implicates many aspects of our physical being in real space.<sup>283</sup> For this reason, according to New Virtualist principles, the embodied information that makes up a person’s virtual self should not be seen as property of the physical self when it comes to privacy protection. Rather, there are two bodies – the one in real space constituted by our physical bodies (which includes our thoughts, emotions, mind, etc.), and the one in cyberspace constituted by information – according to New Virtualism, these two “bodies,”

---

<sup>281</sup> *The Digital Person*, *supra* at note 58, 1.

<sup>282</sup> *Privacy and the New Virtualism*, *supra* at note 277, 226.

<sup>283</sup> *Privacy and the New Virtualism*, *ibid* at 229.

together, to make up an individual's sense of self and personhood.<sup>284</sup>

This is the basis upon which a person's privacy interest in this information should be protected.

This is especially appropriate when it comes to social networking information in the employment relationship. If we conceptualize this information as a "thing" over which an individual has a property right, there is a corresponding likelihood that a person may forfeit an element of that property right through a contract. This is what happens when there are workplace social networking or internet-use policies that state that an employer may monitor all of an employee's computer activity. As was discussed in Chapter 2, one of the key aspects of employment law is to ensure that the freedom of contract does not dominate employment relations – we need to ensure that our societal core values are not compromised and commodified as a result of an inequality in bargaining power. To think of an individual's ability to control the audience of his or her social networking information as an element of personal autonomy rather than an exercise of property rights gives a clearer understanding of the extent to which an employer should be able to monitor an employee's social networking information – this element of personal autonomy will not be surrendered by an employee as a commodity.

---

<sup>284</sup> Privacy and the New Virtualism, *ibid* at 228-229.

Yet another reason I think it is necessary to think of social networking information differently from physical documents containing information is the fact that social networking information, by virtue of existing online, has the potential to be accessed very easily by the use of technology. A diary, for example, is physically kept hidden away in a cupboard or drawer (and often locked). The information on a social networking site is in no way physically protected. As a result, it is of a different nature, and thus presents a different, more serious threat to an individual's privacy.

## **7.7 THE CONCEPTUAL ADVANTAGE**

To link privacy to concepts like autonomy and decision-making for the virtual person is conceptually more simple than to create an additional type of privacy relating to information.<sup>285</sup> While a New Virtualist concept of privacy for virtual persons requires by necessity privacy in information, it only does so because the virtual person is made up of that information; it requires only a theorization about “persons in cyberspace” – a contextualization of privacy, rather than a re-conceptualizing or re-categorization.

Think about it this way. A physical person has certain elements of their life that they choose to share with others to varying degrees. I group our personal information into three categories: (1) that which we

---

<sup>285</sup> *Privacy and the New Virtualism, ibid* at 237.

wish to keep completely private; (2) that which we are willing to share with a certain group of people; and (3) that which we are open to sharing with the entire world.

For the first category, we make a conscious decision to not share this information with anyone. These are personal secrets that we keep inside our own head. We are considered to have a right to keep private whatever is in our head that we do not wish to share with others.<sup>286</sup> While that which is in our mind is “information” in a sense, the protection that is given to our thoughts and memories is not considered to be protected under the categorization of “informational privacy;” rather, the idea that we can keep this information in our own head is more closely linked to values of personal autonomy and decision-making, which constitutes an integral part of our personhood.

For the second category of personal information, we share this information to a limited extent. This information is shared with others under certain conditions. We contour the degree to which we share this information based on the nature of the information itself and the nature of our relationship between oneself and the other person. While we all acknowledge that the other person may ‘blab’ this information to others, we generally operate on an assumption that secrets will be kept – and if they are not, we contour what kind of information we share with that

---

<sup>286</sup> Granted, there are exceptions to this; however, the general point that we are allowed to keep our own secrets holds true.



person in the future. This is just a part of life – anything we share with another person can possibly be repeated to others. This information is not protected in any legal way<sup>287</sup>; however, there are physical limitations to the nature of conversations. When we share this information orally, it is delivered in such a way that it can only be heard by those who are within earshot – our expectations of privacy when having a conversation in the physical world are shaped by our physical surroundings. Similarly, if we share this information with a diary, for example, its potential for discovery by unwanted readers has physical limitations – the diary may be kept in a locked drawer in our home, which makes access physically difficult. Once again, despite the fact that it is “information,” our ability to choose how we share this information is not conceived of as “informational privacy;” it is more truly rooted in the idea of personal autonomy.

With respect to the third category of personal information, it is information that we are willing to share with all. For example, if an individual lists his or her phone number and address in the phonebook, he or she is acknowledging that this information can be received by anyone who has access to a phonebook. In the physical world, we sometimes make things known to all others who care to make even cursory explorations into finding this information – as a result, a person

---

<sup>287</sup> Again, exceptions exist (i.e. solicitor-client privilege); however, the general principle holds true.

has no real privacy interest in this information, but he or she does have the personal autonomy to choose whether to make such a public disclosure.

Now, using the principles of New Virtualism, let us think about these levels of personal information as they are applied to physical people in the context of a virtual person who is made up of the information contained in an individual's social networking account. The information and activity contained in a person's social networking account is the information making up an individual's virtual person that is the subject of this work. The pictures, statuses, profile information, page's "liked," etc., while in the form of "information," pieced together work to create an online embodiment of a person.

With respect to the information in the first category, this information would not be contained on a Facebook page. It may be held somewhere in Facebook's network (i.e. whose profile a person may be searching or accessing and how often), but information that one wishes to keep completely secret would not be accessible by any other user on Facebook. Here, the information is basically the same as thoughts that stay within an individual's mind in the physical world – the decision to not share this information with anyone should be respected as a matter of personal autonomy.

The second category is information that is shared via the social network to some limited extent. This can include anything from photos, statuses, wall posts, private messages, notes, etc. Much like in the physical world, when we share this information with another person there is an inherent risk that this person may go on and share the information with other people, whether it be as an oral re-telling or copying and pasting the message or activity itself. As mentioned above, in the physical world there are physical and spatial limitations that allow an individual to assess his or her surroundings when sharing information with another. These types of physical limitations do not exist in the cyber world; however, using an internalist, New Virtualist perspective, one can see that social networking platforms like Facebook do have privacy settings and passwords that function in a way that is analogous to those spatial and physical limitations in the physical world. As was discussed in Chapter 3, the intended audience for any information that is put on Facebook can vary depending on the individual's privacy settings. For example, if I feel like sharing with someone that I had a terrible day, I could share this information over Facebook in a multitude of ways that have varying degrees of privacy. I could write a status for all of my friends to see; I could write a status that only certain friends could see; I could write a wall post on a friend's wall that all of his or her friends could see; I could write a private

message to someone specific (or a group of people), etc. All of these activities have varying expectations of privacy based on the form of the communication and the privacy configurations of my Facebook account. There is still the risk that what is written can be relayed to others by the audience, but the privacy settings allow the user to control his or her audience in a way that is somewhat analogous to the way we use physical limitations to control our audience when sharing information in the physical world. However, the seemingly endless possibilities that exist in the cyber space and the fact that our perceptions and understanding of degrees of online privacy are not physically sensed in the same way as they are in the physical world, there is an increased possibility of inadvertently sharing information with an unintended audience.

The third category of information would be information that is contained on a Facebook page that can be viewed by anyone with access to Facebook. There is no real expectation of privacy in this information.

What New Virtualism does is provide a fairly straightforward analytical tool for how we should approach privacy issues in cyberspace. Rather than focusing on categorization of privacy interests or the concept of privacy itself, New Virtualist principles focus on the

experience of people in cyberspace, and how privacy ought to work in that context.<sup>288</sup>

It is my position that this conceptualization of privacy in online social networking information would help to maximize the potential benefit we can receive from social networking. If people would be free to use social networking in a pure form, without the worry of unwelcome audience members watching their every move, social networking becomes a very useful forum for people to socialize, learn from one another, and pursue a sense of identity and self-actualization. As a result, I think that New Virtualism's conception of how to approach privacy issues in cyberspace, with its recognition of social networking information constituting personhood, and the focus on personal autonomy as the basis for controlling who can access that information, provides a solid framework for how the issues discussed in Chapters 5 and 6 could be addressed.

---

<sup>288</sup> *Privacy and the New Virtualism*, *supra* at note 277, 249.

## **CHAPTER 8      Application of New Virtualism**

Chapter 5 of this work explored some of the issues with respect to employers requesting or demanding access (to differing degrees) to a job candidate's social networking account. Chapter 6 explored similar issues after the employment relationship is established. This Chapter will see just how the New Virtualist principles of Chapter 7 would work to address the specific problems and issues that were discussed in Chapters 5 and 6.

First – a general comment. Employers are not “villains.” At times in this work it may seem that I have portrayed employers as people who are out to snoop around in their employees' business – this is not at all what I am trying to say. I would contend that many, if not most employers have absolutely no interest in looking through an employee's social networking information. However, with the institution of employment having large inequalities in economic, social, and legal power, I think that there is a temptation and incentive for employers to exploit their situation and infringe upon the rights of their employees. For this reason, I think it is important to regulate the relationship, and an employer's ability to consider an employee's social networking information accordingly.

### **8.1 PRE-EMPLOYMENT**

There were practical and legal issues discussed in Chapter 5 when it comes to employers requesting or demanding<sup>289</sup> access to a candidate's social networking information. As a job candidate only falls under the purview of Employment Standards legislation in very limited circumstances in two Canadian jurisdictions, the main legal issues that arise from social networking background checks are under human rights and privacy legislation. Chapter 5 also discussed the following three levels of invasiveness when it comes to the collection of social networking information: Password (highest level of invasiveness - where an employer requests the candidate's login information so that he or she can go through the candidate's personal account<sup>290</sup>); Public (lowest level of invasiveness – where an employer accesses that which any other Facebook user can access); In-Between (varying degrees of invasiveness – can be anywhere from requesting to be the candidate's "Friend" on Facebook to requesting that the candidate login on a computer and watch as the employer navigates the candidate's social networking site).

---

<sup>289</sup> I will be using the words "requesting" and "demanding" interchangeably when speaking of an employer asking for access to a potential employee's social networking information, as I believe in such a situation a request is practically analogous to a demand.

<sup>290</sup> I would include the use of any screen-capturing or keystroke logging program in this category if the information obtained via the program is used to access the candidate's private social networking information.

With respect to the Password level of invasiveness, it is my opinion that this practice should be impermissible. Using the New Virtualist perspective, the elements of an individual's personhood that are accessible by logging into a person's social networking account are potentially unlimited – not only could the reader find out in-depth information about a prohibited ground of discrimination under human rights law, but the reader can potentially access some of the most intimate and private aspects of an individual's life imaginable. Not only this, but there are numerous alternative ways an employer can access and address relevant elements of a candidate's social networking information; the only reason a password could be required is if the employer is interested in prying into online personhood of the candidate to the most intrusive extent possible. This is in some way analogous to an employer asking a candidate the most intimate and personal questions conceivable. However, for the following reason I contend that it is even more inappropriate than that. If an employer asks a candidate a question that is inappropriate (for example, if the employer asks the candidate his or her religious beliefs)<sup>291</sup>, should the candidate wish to file a human rights complaint, he or she would be able to point directly to the fact that the employer asked that question – by virtue of the question being uttered, the candidate is made aware that the

---

<sup>291</sup> As was mentioned at note 178, if the subject matter of the question is a *BFOR*, the question is not inappropriate.



employer took the candidate's religious beliefs into consideration. When an employer has a candidate's social networking password, he or she can peruse the candidate's account without the candidate having any idea what information was accessed, whether it was considered, etc. – he or she is completely in the dark. The degree to which unbridled social networking account access allows an employer to pry into the life of the employee is not appropriate, and the way in which the employer can look into the information privately allows for relatively easy circumvention of any protection afforded to candidates under human rights or privacy legislation.

For these reasons, I believe that legislation like the proposed Private Member's Bill<sup>292</sup> in Nova Scotia should be implemented. However, the legislation should go beyond where the Nova Scotia Bill appears to go, and be more analogous to the protections afforded to job candidates in Ontario and New Brunswick with respect to lie detector tests. The Nova Scotia Bill prohibits *requiring* a candidate's social networking password – it is my belief that in order to have any practical effect, the Bill must go further and prevent employees from even *requesting* this type of access. This final step is necessary because given the inequality in bargaining power that exists between an employer and a candidate, the candidate could consent to a request solely based on the

---

<sup>292</sup> *Bill no X, supra* at note 183.

dynamics of the situation and not because he or she is actually fine with someone prying into their life to that extent. Finally, there is really no need for an employee to gain such in-depth access to a candidate's personal affairs – any reasonable concerns an employer may have can be practically addressed in a much less intrusive manner.

Yet another reason to not allow this kind of access is to respect the dynamics of the virtual community of Facebook and the people who are a part of that community. As was mentioned in Chapter 3, it is against Facebook's user agreement to allow another person to login to your Facebook account, and in Chapter 4 I made reference to a statement from Facebook's Chief Privacy Officer where she spoke out specifically against employers requesting a job candidate's login information. Facebook users tailor their online activity based on who they have as their Friends and their privacy settings. While users are aware that it is entirely possible for a friend to allow another to login to his or her account and view the user's activity, if this were to become common practice, Facebook would lose any real sense of community and things like "Friends" and privacy settings would become useless – this is likely why Facebook has made such activity a violation of its user agreement. A law prohibiting employers to login to a candidate's social networking account would help to alleviate such concerns among users

of social networking sites and allow them to conduct their activity in the online community with a sense of trust and self-determination.

With respect to the Public level of invasiveness, the candidate is making this information known to anyone who wishes to look into it, and consequently, should not have any legally enforceable privacy interest in said information. In accessing this information, there are certainly concerns on the employer's part with respect to human rights and privacy legislation compliance; however, from the candidate's perspective, he or she has chosen to make these elements of their life a part of the public domain. This is not to say that an employer should be able to use this information in any way it sees fit (i.e. if the candidate's public Facebook page reveals his or her religious beliefs, the employer should not be able to reject the person on that basis)<sup>293</sup>; however, when examining this type of social networking background check from an internalist or externalist perspective, I believe the result is substantially the same – if an employer wishes to access this information, the candidate, in making his or her Facebook page public has acquiesced to anyone with access to Facebook being able to view his or her page.

A real concern here is the possibility of collecting inaccurate information. For employers who fall under the purview of privacy

---

<sup>293</sup> Again, as was mentioned at note 178, this is subject to *BFORs*.

legislation, there is a duty placed on the employer to inform the candidate of any collection of personal information prior to the collection, to ensure the accuracy of the information, and a requirement of direct collection. As a result, I think the danger for collection of inaccurate information is mitigated; however, there still exists a large segment of employers whose activity does not fall under the purview of any privacy legislation. In those jurisdictions there is a very real possibility of the collection of inaccurate information, as the candidate can be completely unaware that any social networking background check is being conducted.

The In-Between level of invasiveness is where things get tricky. This is where the standards and requirements in privacy legislation are the most important. As previously mentioned, the type of activity that would fall under this category are things like requesting to be a candidate's Facebook Friend, or requesting that the candidate sign onto his or her Facebook account and navigate the site while the employer looks on. With the former, the candidate has some control in the situation in that he or she can alter his or her privacy settings to allow the employer to see or not see whatever parts of his or her account that the candidate sees fit. With the latter, while it is somewhat analogous to asking for a candidate's password, it is different in that the candidate is present while the employer looks through the account and knows

exactly which information is being accessed. While the latter is potentially more invasive than the former depending what the employer asks to access, in either situation, the candidate knows exactly what the employer is able to see, alleviating the possibility of certain aspects of a candidate's social networking account being used in the hiring process without the candidate even knowing whether the employer accessed said information.

The real issue here, once again, is whether consent to either such exploration into a candidate's social networking account is reliable as true consent or more just a product of the circumstance of vulnerability or inequality. A way to alleviate this problem is to fix the standard for the circumstances in which a candidate's social networking activity is deemed under privacy legislation to be collectible by an employer. In the employment context, private sector privacy legislation has no requirement that the information collected be directly related to the position for which a candidate is being considered. From an internalist perspective, this should absolutely be the standard for an employer delving into a candidate's life in this way; if it is not directly related to the duties for which the employee is being hired, then, quite frankly, it is a part of the candidate's life that is none of the employer's business. It is not the same as biographical information, or information that can be found on a candidate's résumé. This information is constitutive of an

individual's virtual self, and he or she should only be put under pressure to disclose this information in legitimate circumstances. To request access to the information out of curiosity that is not directly related to the employment relationship should be considered inappropriate. Now, if activity on social networking sites is part of the position for which the candidate is being considered, then it is completely reasonable for an employer to want to review the candidate's activities and competency when it comes social networking. Collection standards like those found in public sector privacy legislation – direct relation to the position – should be the norm across the board. It is only in such a situation that asking a candidate to navigate his or her social networking page in front of the employer could be considered appropriate. This way, the employer has a chance to review information that is relevant to the position for which the candidate is being considered, and it allows the candidate to be the person doing the “clicking,” allowing him or her to be aware of exactly which information the employer is asking to see – thus alleviating issues of proof when it comes to allegations of invasive collection of irrelevant information or a potential human rights complaint. Furthermore, there should be a requirement that the employer notify the candidate prior to the interview this will be happening – this way, the candidate has an opportunity to adjust his or her account accordingly (people like to have

an opportunity to clean their home before having visitors). This is not a stretch, nor is it unduly restrictive on employers – it is appropriately respectful of an individual’s personal information. This should also inform what an employer should reasonably be expected to look into when it comes to a determination of negligence in the hiring process, as was discussed in Chapter 5. Depending on the nature of the position (i.e. a position that incorporates social networking activity), it may be such that an employer should be expected to make explorations into the relevant social networking activity of the candidate; however, the expected extent of those explorations should be limited, and should certainly not go so far as to expect a background check with the Password level of invasiveness.

I feel a need to clarify what was said above with respect to an employer requesting to be a candidate’s Facebook friend being acceptable in certain circumstances. I do not believe there should be an outright ban on an employer requesting to be a candidate’s Facebook friend. I think this is too restrictive – employers and job candidates should be permitted to be Facebook friends if they wish.<sup>294</sup> However, the way in which the request is made is very important. If, for example, there was mention during the interview process that the candidate

---

<sup>294</sup> For example, it may preclude employers from considering any current Facebook friends for an employment position, and it prevents two people who may otherwise wish to be Facebook friends from being so as a result of one being considered by the other for employment.

would be receiving a friend request in a way that implied there is some connection between the friend request and the job, then social networking information should have to be directly related to the job itself. However, even if social networking is not directly related to the job and the candidate nonetheless feels some pressure to accept the friend request, he or she is still able to contour the privacy settings of the friendship in such a way that the employer can see little to none of the information the candidate has put on the site.<sup>295</sup> If, however, a candidate were asked during an interview to accept a friend request from the employer on the spot, he or she would not have an opportunity to alter these privacy settings. For this reason, I think such a practice should not be permitted – the candidate loses any sense of control of his or her privacy configuration of the Facebook friendship. For this reason, whether an employer requesting to be a candidate’s Facebook friend is appropriate can vary depending on the surrounding circumstances.

## **8.2 DURING WORKING HOURS**

As was mentioned in Chapter 5, the increased use of social networking sites by employees presents issues for employers with respect to whether an employee is devoting his or her full time and

---

<sup>295</sup> And there would be no way for the employer to know this unless he or she had access to the account of one of the candidate’s friends who was granted greater access.



attention to his or her duties as an employee during working hours. As a result, there are many approaches an employer can take to ensuring employees are not spending too much (or any) of their working hours on their personal social networking accounts. An employer can install software on the computer that limits the types of web-pages employees can access, or a workplace internet use policy can be drafted and attached to all employment contracts outlining the way in which workplace computers are to be used. The employer should be able to do what is necessary (via software or otherwise) to monitor compliance with workplace policies, but it should stop there. Only when there is an enforced policy in place that states that computers are to be only and exclusively used for work purposes<sup>296</sup> (and the actual workplace practice follows suit) should an employer be able to install software like Screen Capturing or Keystroke Logging programs. Furthermore, if this is the case and the employee does consent to the installation of such programs, the employer should be limited to using these programs only to the extent that is necessary to ensure compliance with the workplace computer-use policy (i.e. to see whether an employee was on his or her social networking site for an extended period of time, and not to see what he or she was doing on the site). The reality is that an employer

---

<sup>296</sup> Whether such a stringent policy should be acceptable at all is certainly a legitimate question; however, this question is beyond the scope of this thesis.

does have a legitimate interest in how an employee spends his or her time during working hours; however, this should not grant the employer any right to pry into the personal affairs of an employee, even if the employee is dealing with those personal affairs at work. As far as the employer's interest in full time and attention goes, he or she should be able to be kept in the loop as to whether an employee is using social networking during working hours, but not kept in the loop as to what the employee is doing while on these social networking sites.

If an employee is using a workplace computer or network to browse the internet, the employer also has an interest in some costs or problems that can come along with such use (i.e. virus protection, bandwidth limits, etc.). Generally, however, these problems do not present themselves by the use of social networking sites, but as is the case with ensuring employees give the employer his or her full time and attention, an employer should only be able to make cursory explorations into what an employee is browsing for troubleshooting purposes – not to simply peruse an employee's online activity.

### **8.3 GENERAL SOCIAL NETWORKING ACTIVITY**

This is not to say that employers do not have any interest in what an employee is doing while on social networking sites – as was discussed in Chapter 6, in certain contexts, employers have an interest

in an employee's social networking activity regardless of the physical location in which the person is conducting said activity.

Workplace policies can be written with respect to how employees are to conduct themselves on social networking sites; however, once again, the real issue is the extent to which the employer should be able to monitor the employee's social networking activity in the name of protecting those interests. And while the aforementioned technological means for an employer to gain access to an employees social networking account do exist, it is my position that the employer should not be able to be use these kinds of technological means that are especially available to him or her as an employer to at all times creep the content of what an employee is doing on his or her social networking account, even if it is in the name of protecting a legitimate interest.<sup>297</sup>

Think of it as if the employee was acting in the physical world, as opposed to online. An employer is neither physically able to watch everything an employee does, nor hear everything an employee says. For example, if an employee is cursing his or her employer's name (and thus, damaging the employer's reputation), the chances of an employer finding out about it can increase or decrease depending on certain

---

<sup>297</sup> Once again, an exception to this is situations in which the social networking activity is itself part of the employee's job. In this case, the standard should be, like at the pre-employment phase, that the employer is able to monitor this activity to the extent that is necessary to the operation or program of the institution.

factors. If the employer is present, then it is likely they will see or hear it. If the employee is in a very busy public place, there is a greater likelihood that someone may hear him or her and relay the information to the employer. Even if the employee is speaking with only one co-worker, there is a possibility that the co-worker may relay the information to the employer – this is certainly a risk taken by the employee. However, in the physical world, the employee has a certain level of control in managing these risks – there exist spatial, acoustic, and territorial boundaries, and he or she is able to choose his or her audience based on the existence of these boundaries and control the content of what he or she is saying based the degree to which he or she trusts the audience he or she has. An individual’s ability to make these decisions for oneself is considered to be part of an individual’s right to personal autonomy.

When thinking of it from an internalist perspective, the employee is navigating within the social networking site’s boundaries. When an employee writes something on his or her Facebook page (for example, something that damages his or her employer’s reputation), the way he or she is navigating the site is that he or she is producing this information under the understanding that he or she has placed certain technological privacy limitations on the audience that can receive this information. In this regard, the privacy settings of the employee’s social

networking account must be respected – if the employer is not a part of that intended audience, this should be respected. Now, this is not to say that because the statements were written online, the employee should be somehow immune from facing any real-world consequences if the employer were to find out – that would be the Legal Immunity Thesis of the original Virtualist idea that existed in an era of online activity gone by. What New Virtualism would dictate is that while the individual’s decision to write such statements on Facebook with particular privacy settings should, for the most part, be respected as a matter of personal autonomy (and the employer should generally be precluded from invading into the employee’s personal life without good reason), it is recognized that the borders between the online world and the physical world are permeable. And by putting this information out into the online world, the employee is certainly taking a risk that someone may relay this information to the employer either orally or electronically, and this could very well have consequences for the employee in the physical world. In this case, the employer should be able to react to social networking activity of employees – and the employer can only react if he or she knows that the activity occurred.

What I mean by all of this is that employers should not be able go on “fishing expeditions,” or have a policy that they may simply monitor an employee’s social networking activity at all times. However, if the

employer has legitimate, reasonable grounds to believe that an employee is engaging in some social networking activity that affects the interests of the employer (i.e. writing defamatory statuses about the employer for all of his or her Facebook friends to see, and one of those friends told the employer about it), there should be a way for the employer to access this information. One way is for the employer to make inquiries in the physical world that do not involve the employer intruding upon the privacy of the employee via technological means (i.e. Screen Capturing or Keystroke Logging programs). The employer could ask people whom he or she knows to be the employee's Facebook friend about the employee's activity. The employer can ask that one of the employee's Facebook friends copy and paste the employee's Facebook activity to him or her. This is completely reasonable. There is, however, a wrinkle to this process. If the employer is asking this information from another one of his or her employees, asking is a delicate issue that, in the situation, may be more akin to coercion. As such, the employer should be able to ask other employees about the alleged activity (just as he or she can ask one employee about another employee's activity in the physical world), but the employer should be precluded from asking that an employee copy and paste or actually show the alleged activity to the employer. This does not adequately respect that employee's autonomy in his or her own social networking

account. Now, if the employee decides himself or herself to show the activity of the other employee to the employer, this is acceptable, as it is part of the risk Facebook users assume when posting information for other Facebook users to see – some of those users may relay that information to unwanted audiences. So how, and from whom, the employer retrieves the information is very important. This is the kind of explorations that is not currently happening during examinations of employment law issues arising out of social networking activity – there needs to be an assessment of the appropriateness of the manner in which the information was accessed.

Despite an employer's best efforts to gain access to the information, he or she may come away from these explorations empty-handed, and the only way for the him or her to look into the Facebook activity of the employee is through the aforementioned technological means. In such circumstances, this should be allowed in limited circumstances, and I can see two possible ways to go about allowing this.

The first is an ex post facto assessment. If the employer has legitimate, reasonable grounds to believe that the employee is engaging in social networking activity that is detrimental to the interests of the employer, the employer is then permitted to use technological means (i.e. Keystroke Logging or Screen Capturing programs) to view the

social networking activity of the employee. In an effort to ensure that employers are not simply creeping an employee's Facebook activity as a form of fishing expedition, when there is an employment law issue arising out of an employee's social networking activity, the court or board hearing the issue needs to engage in discussion and analysis of the way in which the employer obtained the information at issue. Key to this analysis will be whether the employer had a reasonable, legitimate reason to infringe upon the employee's expectation of privacy. It is my belief, however, that this approach is not effective for the following reason: the only way the employer's reasonable grounds for prying into the social networking activity of the employee will be examined is if it turns out that the employee's activity was grounds for discipline, and the employee challenges that discipline. But what about situations in which the employer was incorrect, and the employee has not actually engaged in such social networking activity? Yes, there will be no discipline in such a situation, but the privacy infringement will still have occurred. This opens up the possibility of more privacy infringements. For this reason, I do not believe this approach adequately protects the employee's privacy interests in his or her social networking activity.

Once privacy is violated, it cannot be regained, and to monitor someone's social networking activity in this way (via technological



means without their knowledge or consent) is not unlike a wiretap. For this reason, I believe that in order for an employer to use technological means like Keystroke Logging or Screen Capturing programs to monitor an employee's social networking activity, the employer must receive prior authorization from some independent body (e.g. a Labour Relations Board). To receive prior authorization from the independent body, the employer must be able to demonstrate that he or she has reasonable, legitimate grounds to believe that the employee is engaging in social networking activity that is worthy of discipline. Furthermore, the authorization given by the independent body could appropriately limit the scope and extent to which the employer can look into the employee's social networking activity. The way the independent body would make the determination of whether to authorize the monitoring would be analogous to the way the Supreme Court of Canada treats admissibility of any records in which an individual has a reasonable expectation of privacy, such as personal diaries. In determining when it is reasonable to demand access to said information, the court engages a balancing act that involves an assessment of the individual's reasonable expectation of privacy and a weighing of that expectation against the legitimate need to interfere therein.<sup>298</sup> In my opinion, this is the most effective

---

<sup>298</sup> See *M(A) v Ryan*, [1997] 1 SCR 157 at paragraph 89-102, where the balancing test from *R. v O'Connor*, [1995] 4 SCR 411 is applied to civil proceedings.

way to protect the employee's privacy interest in his or her social networking activity, but still respect the fact that an employer may need to access this information in certain circumstances.

What this amounts to is that the employer, if he or she finds out that such activity was conducted by an employee on a social networking site, should be able to respond to that activity appropriately; however, the law should certainly respect and protect the individual's right to engage in social networking activity with the privacy contours of his or her choice as a matter of personal autonomy – within reason, the employee should be able to choose his or her audience.

This is the extent to which social networking activity should be protected in the employment relationship – it should generally (not absolutely) be protected from unwanted and unwelcome employee monitoring on the part of the employer, but the employee should not be immune from the consequences that can result from participating in social networking activity. This approach respects the reasonable privacy expectations individuals choose when they participate in social networking, it frees them to express themselves online without fear of constant supervision from their employer, and it respects the employer's legitimate right to react should an employee do something that is detrimental to the employment relationship. This is the balanced social networking environment we want – a virtual space where we can feel

secure to express ourselves and socialize as we see fit, but one that is still connected to the civilized, physical world in which we live.

## **CHAPTER 9      Conclusion**

As use of technology and the use of social networking increases, the risk presented to personal privacy correspondingly increases. When it comes to the protection of an individual's privacy interest in his or her social networking information in the employment context, we are not doing a very good job.

At the pre-employment phase, Employment Standards Acts do not protect job candidates, except in very limited circumstances. Human rights and labour relations legislation, while they do extend to protect certain interests of job candidates, have significant issues with respect to proof when it comes to their practical efficacy in preventing employers from engaging in discriminatory or unfair labour practices as a result of social networking background checks. Even legislation proposed specifically with the goal of protecting job candidates from being subject to unwanted social networking background checks at the Password level of invasiveness do not appropriately take consent concerns into account.

The privacy legislation that is supposed to govern the extent to which an employer can collect social networking information about an employee or candidate is insufficient. First of all, its jurisdictional application is minimal. There exists legislation that regulates the

collection, use, and distribution of information for employees or candidates in federally regulated industries, the public sector, the provincially regulated private sector in Alberta, BC or Quebec, and the legislated tort of invasion of privacy protects citizens in BC, Manitoba, Saskatchewan, and Newfoundland and Labrador to a very limited degree; however, those in the provincially regulated private sector outside of these jurisdictions receive no statutory privacy protection whatsoever. Second, it is only in the public sector that the social networking information collected by an employer must be directly related to the employee or candidate's job. In the aforementioned statutes in Alberta and BC, there is no requirement that the employer receive the consent of the employee or candidate before collecting this information, and in all other privacy legislation applicable to the private sector (including the tort of invasion of privacy), the standard of what can be collected is a vague standard of "reasonableness." For all of those not protected by specific privacy legislation, there exists only the tort of "intrusion upon seclusion," which only protects an individual from such intrusions that are highly offensive causing distress, humiliation, or anguish. Considering the amount and nature of information that is contained in an individual's social networking account, this is insufficient protection.

When it comes to employment law disputes arising out of the use of social networking, arbitrators, courts and legal scholars are focused on the application of first principles of employment law to the social networking activity in question, and not addressing and analyzing the privacy issue that is at stake – the creeping by the employer of the employee’s social networking activity. Rather, computer use policies are being relied upon by employers as a form of consent from the employee to allow the employer to monitor the employee’s computer activity. There has not been nearly enough consideration of the potential invasiveness of such a practice, and considering the interest the employer is seeking to protect, the reasonable limits that should be placed on an employer’s ability to monitor what an employee does on his or her work computer, or social networking sites generally.

Social networking is a use of technology that is very intimately connected to a person’s sense of individuality and identity. If it is to present any real benefit to individuals and society as a whole (and I think that it has great potential in this regard), it needs very careful and functional privacy protection. Despite the problems that exist with our current approach, I think there is still a way for us to create an environment where people can use social networking to its full potential and privacy concerns are effectively mitigated. To do so, however, requires a change in how we perceive social networking information.

Treating social networking information like property, and protecting it by giving individuals a right to “informational privacy’ is the wrong approach. This has only led to an approach that does not effectively take into account the complicated dynamics of the employment relationship. In this work I have attempted to argue that the principles of New Virtualism are a more appropriate conceptual basis upon which we should address this issue going forward.

While New Virtualist principles provide a roadmap for the general, conceptual direction we should take in addressing this issue, the specific means to achieve the best regulation (be it, for example, specific legislation, changes to Employment Standards legislation, or the development of the common law) could be the subject of further study and exploration – this is the next step. The first step to finding a solution, however, is acknowledging that a problem exists. And when it comes to the privacy protection afforded to social networking information in the context of the employment relationship, a problem certainly exists.

## BIBLIOGRAPHY

### LEGISLATION

- Access to Information and Protection of Privacy Act*, SNL 2002, c A-1.1.
- An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*, RSQ, c A-2.1.
- An Act Respecting the Protection of Personal Information in the Private Sector*, RSQ, chapter P-39 1.
- Bill No. X (as introduced), *An Act to Amend Chapter 246 of the Revised Statutes, 1989*, the *Labour Standards Code*, 4<sup>th</sup> Session, 61<sup>st</sup> General Assembly, Nova Scotia, 61 Elizabeth II, 2012, Private Member's Bill, Andrew Younger, MLA for Dartmouth East.
- Canadian Charter of Rights and Freedoms*, R.S.C, 1985 Appendix II, No. 44 s. 8.
- Canadian Human Rights Act*, RSC 1985 c H-6.
- Constitution Act, 1867*, 30 & 31 Vict, c 3.
- Criminal Code of Canada*, RSC 1985, c C-46, as amended.
- Employment Standards Act*, SO 2000 c 41.
- Employment Standards Act*, SNB 1982, c E-7.2.
- Employment Standards Act*, RSBC 1996 c 113.
- Employment Standards Code*, RSA 2000, c E-9.
- Freedom of Information and Protection of Privacy Act*, RSA 2000, c F-25.



*Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165.

*Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31.

*Freedom of Information and Protection of Privacy Act*, RSPEI 1988, c F-15.01.

*Freedom of Information and Protection of Privacy Act*, SNS 1993, c 5.

*Freedom of Information and Protection of Privacy Act*, SS 1990-91, c F-22.01.

*Labour Relations Act*, R.S.N.L. 1990, c. L-1.

*Labour Standards Act*, RSS 1979 c L-1.

*Occupational Health and Safety Act* R.S.O. 1990.

*Ontario Human Rights Code*, RSO 1990, c H.19.

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

*Personal Information Protection Act*, SA 2003 c P-6.5.

*Personal Information Protection Act*, SBC 2003 c 63.

*Privacy Act*, RSBC 1996, c 373.

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

*Privacy Act*, RSNL 1990 c-P22.

*Privacy Act*, RSS 1978, c P-24.

*Right to Information and Protection of Privacy Act*, SNB 2009, c R-10.6.

*The Freedom of Information and Protection of Privacy Act*, CCSM c F175.

*The Privacy Act*, CCSM c P125.

*Trade Union Act*, RSNS 1989, c 475

*Trade Union Act*, RSS 1978, c T-17.

## **JURISPRUDENCE**

*Alberta Distillers Ltd. v. United Food and Commercial Workers, Local 1118* [2009] AGAA No 46.

*BDC v BJB* [2012] YJ No 91.

*British Columbia (Public Service Employee Relations Commission) v. British Columbia Government and Service Employees' Union (B.C.G.S.E.U.)* [1999] S.C.J. No. 46.

*Canada Post Corp v Canadian Union of Postal Workers*, [2012] CLAD No 85 (Ponak).

*Chatham-Kent (Municipality) v. National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada), Local 127* (Clarke Grievance), 159 LAC (4th) 321, [2007] OLAA No 135 (Williamson) (QL).

*Cottrell v Manitoba (Workers Compensation Board)* [1997] MJ No 249 (Man QB).

*DD v HA* [2008] BCHRTD No 361.

*EV Logistics v. Retail Wholesale Union, Local 580 (Discharge Grievance)*

[2008] BCCA No 22 (Laing).

*FA v Deputy Head (Department of Citizenship and Immigration)* 2011

PSLRB 100 [*Andrews Grievance*] (Rogers).

*Health Sciences Association of British Columbia v Fraser Health*

*Authority (Surrey Memorial Hospital)* [2011] BCCAAA No 125

(Glass).

*Jones v Tsige*, [2011] OJ No 1273.

*Jones v Tsige*, 2012 ONCA 32.

*K (SJ) v Chapple*, [1999] SJ No 186, (Sask QB).

*Lougheed Imports Ltd. (West Coast Mazda) v. United Food and*

*Commercial Workers International Union, Local 1518*, 2010

CanLII 624482 (BCLRB).

*M(A) v Ryan*, [1997] 1 SCR 157.

*Ontario Public Service Employees Union v Ontario (Ministry of*

*Community and Social Services)* [2011] OGSBA No 167 (Johnston).

*Pierre v Pacific Press Ltd*, [1994] B.C.J. No. 583 (BCCA).

*R. v O'Connor*, [1995] 4 SCR 411.

*R v Tessling*, 2004 SCC 67, [2004] 3 SCR 432, 244 DLR (4<sup>th</sup>) 541.

*Re Ford Motor Co of Canada Ltd. and UAW, Local 200* (1964), 15 LAC

349n (Lang).

*Re Inco Metals Co and United Steelworkers*, [1978] OLAA No 2, 18 LAC  
(2d) 420 (Weatherill).

*Re Madame Vanier Children's Services and Ontario Public Service*

*Employees' Union*, [1988] OLAA No 2, 5 LAC (4th) 225 (Verity).

*Re United Auto Workers, Local 444 and Chrysler Corp of Canada*, [1961]

OLAA No 1, 11 LAC 152 (Bennett).

*Re United Food and Commercial Workers Union, Local 1000A and*

*Janes Family Foods (Surveillance Grievance)*, [2006] O.L.A.A. No.

611 (Trachuck) (QL).

*Somwar v McDonald's Restaurants of Canada* [2006] OJ No 64.

*St Mary's Hospital v. HEU*. (1997) 64 LAC (4th) 250 (BC) [Larson].

*Trout Point Lodge Ltd v Handshoe* [2012] NSJ No 427.

*Walker v British Columbia College of Dental Surgeons*, [1997] BCJ No

433 (BCSC).

## **SECONDARY MATERIALS**

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

Alberta Office of the Information and Privacy Commissioner, *Order*

*F2012-07* – Calgary Police Service (20 April 2012) online:

<<http://www.oipc.ab.ca/downloads/documentloader.ashx?id=3050>>.

Allen Linden, Bruce Feldthusen et al, "Negligence" *Halsbury's Laws of*

*Canada*, (2012) online (QL).

- Andreas Kaplan, Michael Haenlein, “Users of the World, Unite! The Challenges and Opportunities of Social Media” (2010) *Business Horizons* 53(1).
- Andela Swan, Jakub Adamski et al, “Contracts” *Halsbury’s Laws of Canada* (2012) online (QL) at HCO-64.
- Brian Langille, “Labour Law is a Subset of Employment Law” (1981) 31:2 UTLJ 200.
- Brian Langille, “Labour Policy in Canada: New Platform, New Paradigm” (2002) 28 *Can Pub Pol’y* 133.
- Danah Boyd and Nicole Ellison, “Social Network Sites: Definition, History, and Scholarship” (2008) *Journal of Computer-Mediated Communication* 13, 210-230.
- Daniel Solove, “A Taxonomy of Privacy” (2006) 154 *U Pa L Rev* 477.
- Daniel Solove, *The Digital Person: Technology and Privacy in the Information Age*, (New York: NYU Press 2004).
- David Beatty, “Labour is Not a Commodity” in Barry Reiter & John Swan, eds., *Studies in Contract Law* (Toronto: Butterworths, 1980) 313.
- David R Johnson and David Post, “Law and Borders: The Rise of Law in Cyberspace” (1996) 48 *Standord Law Review* 1367.
- Françoise Baylis, “The Self *in Situ*: A Relational Account of Personal Identity” in *Being Relational: Reflections on Relational Theory in Health Law* (Vancouver: UNC Press, 2012).

- Geoffrey England et al, "Employment" *Halsbury's Laws of Canada* (2011 Reissue) online (QL).
- Ilana Gershon, "Un-Friend My Heart: Facebook, Promiscuity, and Heartbreak in a Neoliberal Age" (2011) 84 *Anthropological Quarterly* 865.
- James Grimmelman in "Virtual Borders: The Interdependence of Real and Virtual Worlds" *First Monday* (6 February 2006) online: <[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=868824](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=868824)>.
- Janis L Goldie, "Virtual Communities and the Social Dimension of Privacy" (2006) 3:1 *UOLTJ* 133.
- Jennifer Nedelsky, "Reconceiving Autonomy: Sources, Thoughts, and Possibilities" (1989) 7 *Yale JL & Feminism* 7.
- Jocelyn Downie and Jennifer Llewellyn, eds, *Being Relational: Reflections on Relational Theory in Health Law* (Vancouver: UNC Press, 2012).
- Jonathon Penney "Privacy and the New Virtualism" (2008) 10 *Yale J L & Tech* 194.
- Jonathon Penney, "Understanding the New Virtualist Paradigm" (2009) *Journal of Internet Law* 12.
- Labour Law Casebook Group, *Labour and Employment Law: Cases, Materials, and Commentary*, (Toronto: Irwin Law: 2004) 7<sup>th</sup> ed.

- Liman Pinar Tosun, "Motives for Facebook Use and Expressing "True Self" on the Internet" (2012) 28 *Computer in Human Behavior* 1510.
- Michael Power et al, "Access to Information and Privacy" *Halsbury's Laws of Canada* (2011 Reissue) online (QL).
- Orin Kerr, "Enforcing Law Online" (2007) 74 *U Chi L Rev* 745, 745, 751.
- Orin Kerr, "The Problem of Perspective in Internet Law" (2003) 91 *Geo LJ* 357.
- Priscilla Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (Chapel Hill: The University of North Carolina Press, 1995).
- Raymond Edward Pahl, "Editor's Introduction: Historical Aspects of Work, Employment, Unemployment and the Sexual Division of Labour" in Raymond Edward Pahl, ed., *On Work: Historical, Comparative and Theoretical Approaches* (Oxford: Basil Blackwell, 1988).
- Robert Sprague, "Rethinking Information Privacy in an Age of Online Transparency" (2008) 25 *Hofstra Lab & Empl J* 395.
- Rosanne Lienhard, "Negligent Retention of Employees: An Expanding Doctrine" (1996) 63 *Def Couns J* 389.
- Susan Sherwin, "A Relational Approach to Autonomy in Health Care" in *Feminist Health Care Research Network*, Susan Sherwin,

coordinator, *The Politics of Women's Health: Exploring Agency and Autonomy* (Philadelphia, PA: Temple University Press, 1998).

WJ Wilson, "When Work Disappears: New Implications for Race and Urban Poverty in the Global Economy" (1999) *Ethnic and Racial Studies* volume 22 number 3.

## **OTHER SOURCES**

Andy Kazeniak, "Social Networks: Facebook Takes Over Top Spot,

Twitter Climbs" *CompetePulse* (9 February 2009) online:

<<http://blog.compete.com/2009/02/09/facebook-myspace-twitter-social-network/>>.

David Doorey, "Can an Employer ask a Job Applicant for their Facebook

Password?" *Doorey's Workplace Law Blog: Thoughts on Canadian*

*Labour & Employment Law for Students & Others* (20 March 2012)

online: <<http://www.yorku.ca/ddoorey/lawblog/?p=4995>>.

Erin Egan, *Protecting Your Passwords and Your Privacy* (23 March

2012) online: Facebook

<[https://www.facebook.com/note.php?note\\_id=326598317390057](https://www.facebook.com/note.php?note_id=326598317390057)>.

EcecuNet "Why #Jobseekers MUST Manage Their Online Reputation"

*Career Chaos* (1 March 2010) online:

<[http://coachmeg.typepad.com/career\\_chaos/2010/03/why-jobseekers-must-manage-online-reputation.html](http://coachmeg.typepad.com/career_chaos/2010/03/why-jobseekers-must-manage-online-reputation.html)>.



Facebook “Data Use Policy” online:

<<http://www.facebook.com/about/privacy/>>.

Facebook “Help Center” online: <<http://www.facebook.com/help/>>.

Facebook “Main Page”online: <<http://www.facebook.com/>>.

Facebook “Mission Statement” online:

<<http://www.facebook.com/facebook/info>>.

Facebook “Principles” online:

<<http://www.facebook.com/principles.php>>.

Facebook “Statement of Rights and Responsibilities” online:

<<http://www.facebook.com/legal/terms>>.

Information and Privacy Commissioner (Ontario), *Reference Check: Is*

*Your Boss Watching? The New World of Social Media: Privacy and Your Facebook Profile* (April 2012), online:

<<http://www.ipc.on.ca/images/Resources/facebook-refcheck.pdf>>.

John Perry Barlow, *A Declaration of the Independence of Cyberspace*

(1996) online:<[https://projects.eff.org/~barlow/Declaration-](https://projects.eff.org/~barlow/Declaration-Final.html)

[Final.html](https://projects.eff.org/~barlow/Declaration-Final.html)>.

Morgan Campbell, “Would you reveal your Facebook password for a job?” *The Toronto Star* (20 March 2012) online:

<<http://www.thestar.com/business/article/1148973--would-you-reveal-your-facebook-password-for-a-job>>.

Nicholas Carlson, "Facebook Now Has 901 Million Monthly Users, With 526 Million Coming Back Every Day" *San Francisco Chronicle* (2 May 2012) online: <<http://www.sfgate.com/cgi-bin/article.cgi?f=/g/a/2012/04/23/businessinsiderfacebook-now-has-900.DTL>>

Ontario Human Rights Commission, "Statement regarding employers asking for Facebook passwords," (23 March 2012) online: <<https://facebook.com/the.orhc/posts/320570581329371>>.

Provincial and Territorial Privacy Commissioners and Ombuds Office, "Memorandum of Understanding" (November 2011) online: <[http://www.priv.gc.ca/au-ans/mou\\_e.asp](http://www.priv.gc.ca/au-ans/mou_e.asp)>.

Robert Todd, "Facebook is the New Water Cooler: B.C. Ruling Shows Venting on Online Social Media Sites Can Lead to Getting Fired", *Canadian Lawyer Magazine* (February 2011) 39, 41.

Rosemary Haefner, "More Employers Screening Candidates via Social Networking Sites" *Careerbuilder* (10 June 2009) online: <<http://careerbuilder.com/Article/CB-1337-Getting-Hired-More-Employers-Screening-Candidates-via-Social-Networking-Sites/>>.

Ruchi Sangvhi, "Facebook Gets a Facelife" *The Facebook Blog* (5 September 2006) online: <<http://blog.facebook.com/blog.php?post=2207967130>>.

*The Sydney Morning Herald* “It’s Akin to Requiring Someone’s House Keys: Employers Ask Job Seekers For Facebook Passwords” (21 March 2012) online: <<http://www.smh.com.au/technology/technology-news/its-akin-to-requiring-someones-house-keys-employers-ask-job-seekers-for-facebook-passwords-20120321-1vioi.html>>.

The Office of the Information and Privacy Commissioner for British Columbia, *Guidelines for Social Media Background Checks* (October 2011), online: <<http://www.opic.bc.ca/pdfs/private/guidelines-socialmediabackgroundchecks.pef>>.

The Office of the Information and Privacy Commissioner’s of British Columbia. “Summary of the Office of the Information and Privacy Commissioner’s Investigation of the BC NDP’s use of social media and passwords to evaluate candidates” P11-01-MS, online: <[http://www.oipc.bc.ca/Mediation\\_Cases/PDFs/2011.P11-01-MS.pdf](http://www.oipc.bc.ca/Mediation_Cases/PDFs/2011.P11-01-MS.pdf)>.

The Office of the Privacy Commissioner of Canada “Facebook agrees to address Privacy Commissioner’s concerns” (27 August 2009 (online): <[http://www.priv.gc.ca/media/nr-c/2009/nr-c\\_090827\\_e.asp](http://www.priv.gc.ca/media/nr-c/2009/nr-c_090827_e.asp)>.

The Office of the Privacy Commissioner of Canada “Privacy Commissioner completes Facebook review” (22 September, 2012)

online: <[http://www.priv.gc.ca/media/nr-c/2010/nr-c\\_100922\\_e.asp](http://www.priv.gc.ca/media/nr-c/2010/nr-c_100922_e.asp)>.

The Office of the Privacy Commissioner of Canada “Privacy Commissioner: Facebook shows improvement in some areas, but should be more proactive on privacy when introducing new features” (4 April 2012) online: <[http://www.priv.gc.ca/media/nr-c/2012/nr-c\\_120404\\_e.asp](http://www.priv.gc.ca/media/nr-c/2012/nr-c_120404_e.asp)>.

The Office of the Privacy Commissioner of Canada “Privacy Commissioner launches new Facebook probe” (27 January 2012) online: <[http://www.priv.gc.ca/media/nr-c/2010/nr-c\\_100127\\_e.asp](http://www.priv.gc.ca/media/nr-c/2010/nr-c_100127_e.asp)>. *The Oxford English Dictionary*, 2d ed, *sub verbo* “privacy”, online: Oxford English Dictionary <<http://www.oed.com>>.

Tina Giesbrecht and Roland Hung, “Are Employers in British Columbia and Alberta stepping outside privacy boundaries in requesting access to a job applicant’s social media profile?” *McCarthy Tetrault Publications* (5 April 2012) online: <[http://www.mccarthy.ca/article\\_detail.aspx?id=5814](http://www.mccarthy.ca/article_detail.aspx?id=5814)>.

Todd Wasserman, “83 Million Facebook Accounts Are Fake” *Mashable Social Media* (2 August 2012) online: <<http://mashable.com/2012/08/02/fake-facebook-accounts/>>.