THE RIGHT TO BE FORGOTTEN: NO SOLUTION TO THE CHALLENGES OF THE DIGITAL ENVIRONMENT

by

Jordan Levesque

B.Com., The University of Auckland, 2012

LL.B. (Honours), The University of Auckland, 2012

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF LAWS

in

THE FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES

(Law)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

August 2016

Abstract

The right to be forgotten was introduced into the EU with great passion and enthusiasm as a new dawn in privacy protection on the Internet. This thesis challenges this and argues that the current drafting of the right to be forgotten found in the *Regulation* is a partial solution only. It argues that Article 17, which empowers private businesses to remove content from the Internet is a step that must be exercised with caution. This thesis explores current understandings of privacy and discusses the value privacy has to individuals and societies while examining how this is changing under ever-growing Internet culture. This thesis contains a comparative assessment of privacy protection offered in Canada and New Zealand and discusses how the right to be forgotten goes far beyond what is currently being offered in these chosen jurisdictions. Using the decision of *Google Spain* the thesis illustrates how continued application of the right to be forgotten will create real problems for fundamental human rights such as freedom of expression and privacy on the Internet. This thesis highlights 3 key problems created by the right to be forgotten as presenting a real risk of Internet censorship, devaluing privacy, and a complete absence of a unified jurisdiction to enforce the *Regulation.* This thesis argues that such problems cannot be overlooked as they risk damaging the much celebrated openness and freedom of the Internet. As an answer to the highlighted problems, this thesis proposes amendments to the *Regulation* that will temper the current inadequacies found in the right to be forgotten. This thesis proposes amending the *Regulation* to introduce a co-regulatory corporate social responsibility regime that can promote transparency and due process within any right to be forgotten request. It also proposes including a remedial process within any right to be forgotten request to ensure fundamental human rights are not overlooked by private business. Finally, this thesis proposes

amending the right to be forgotten to include a re-shaped reasonable expectation of privacy assessment that will ensure the right to be forgotten aligns with how individuals perceive and value privacy on the Internet.

Preface

This is thesis is the original, unpublished, independent work by the author.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

AEPD:	Agencia Española de Protección de Datos.
BCCA:	Court of Appeal of British Columbia.
BCSC:	Supreme Court of British Columbia.
BORA:	New Zealand Bill of Rights Act 1990.
CSR:	Corporate Social Responsibility.
CJEU:	Court of Justice of the European Union.
DMCA:	The Digital Millennium Copyright Act.
EU:	European Union.
ICCPR:	International Covenant on Civil and Political Rights.
PCC:	Press Complaints Commission.
PIPA:	Personal Information Protection Act.
PIPEDA:	Personal Information Protection and Electronic Documents Act.
SNWs:	Social Networking Websites.

Glossary

Digital Natives:	Refers to individuals who have been brought up in the age of digital technology and therefore familiar with computers and the Internet.
Geo-blocking:	A form of Internet censorship where content is blocked based upon the physical location of the user.
Keystroke:	A single depression of a keyboard.
Top-level domain:	The highest domain level in the Domain Name System. Top-level domains typically refer to a specific country. For example, ".ca" is the top-level domain within Canada.
Web 2.0:	The second wave of Internet culture and represents an Internet where there is an emphasis on user-generated content.

Acknowledgements

I am thankful to the faculty, staff and students at UBC. I owe particular thanks to Anthony Sheppard, whose thoughtful discussion and questions guided this work. I would like to thank Shigenori Matsui for his support and teaching that deepened my understanding in this field. I would also like to thank Dr. Luciana Duranti for her support throughout my research. Finally, I would like to acknowledge my family and friends for their continued support and love.

Dedication

Ka mura, Ka muri

Chapter 1: Introduction

> The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress far greater than could be inflicted by mere bodily injury.[1]

Privacy as a concern remains as relevant as it was when authors Warren and Brandeis published their article "The Right to Privacy*"* in 1890.[2] The context has surely changed, but the problem remains. Privacy as an individual right or value demands protection. Yet little evidence exists reflecting a parallel between the need for protection and the available safeguards. In particular, the latest safeguard—found in the right to be forgotten—fails to protect privacy with reckless disregard for essential legal values and important attributes of the Internet. This thesis will argue that the right to be forgotten must be amended in order to effectively achieve its goal of providing control to individuals' personal information on the Internet. Currently, the right to be forgotten cures the symptoms of an unauthorized privacy disclosure but does not align with social expectations of privacy. Amending the right to be forgotten will avoid corporate censorship, ensure that its protection aligns with societies expectation of privacy and enable unified jurisdictional reach.

---

[1] Samuel Warren & Louis Brandeis, "The Right to Privacy" (1890) 4:5 Harv L Rev 193.
[2] *Ibid*.

The Internet is a universal and integral part of daily life in Western society. Connectedness to the Internet is constantly increasing and interactions with the Internet also continue to grow. As the Internet becomes more pervasive, how the law regulates and mediates the Internet becomes increasingly important. The Internet, as we know it, has been accessible for 3 decades and has created, supported and facilitated a raft of social and individual changes for those who are connected with it. While many changes have been positive,[3] the Internet has also challenged traditional legal values by easing their circumvention. It is able to challenge legal concepts that are made in the tangible world because it does not operate within the tangible world. The Internet can be everywhere without occupying physical space.

This thesis will examine the right to be forgotten as introduced by the European Commission to the European Union (the *EU*) (the *Regulation*[4]) and argue that such a right does not fully remediate unauthorized disclosure of personal information. The focus of this thesis is on the challenge created by the unauthorized disclosure of personal information on the Internet and the remedies developed to stifle such undesirable behaviour. In particular, this thesis will consider the right to be forgotten, a tool developed in an attempt to regulate the Internet by preventing the widespread dissemination of personal information.

---

[3] Gadi Wolfsfeld, "Social Media and the Arab Spring: Politics Comes First" (2013) 18:2 The International Journal of Press/Politics 115 (In 2011 Arab nations united through social media platforms to organise individuals and events that dominated the 'Arab Spring' throughout Eqypt, Libya, Syria, Yemen, Bahrain, Saudi Arabia and Jordan).

[4] EC, *Commission Regulation (EU) 679/2016 of the European Parliament and of the Council of 27 April 2016 on the protection of natural person with regard to the processing of personal data on the free movement of such data, and repealing Regulation 95/46/EC (General Data Protection Regulation),* OJ, L 119/1.

The essence of the right to be forgotten is the ability of individuals to request that personal information be removed from search results displayed through Internet search engine operators, such as Google, Bing and Yahoo.[5] The right to be forgotten is an outcome of an update to *Regulation* 95/46/EC of the European Parliament and of the Council (the *1995 Regulation*).[6] Under the *1995 Regulation*, individuals had a right to erasure that was bundled with the other remedial actions of blocking and rectifying.[7] As the right to erasure was buried within other corrective acts, it was rarely invoked. The *Regulation* has carved the right to erasure out as a separate action within the EU data protection legislation giving the right its own platform and a new name as the right to be forgotten.[8] Article 17 of the *Regulation* provides individuals (data subjects[9]) with the right to make the Internet 'forget' something about them. Under the approach being established by the *Regulation*, an individual has the right—among others—to request that information be removed if the information is personal data and is no longer necessary.[10]

Although the *Regulation* provides individuals with the chance to have something about them forgotten, the *Regulation* can achieve this only to the extent that the information is disclosed through a search engine website.[11] Importantly, for this thesis, the *Regulation* does not require

---

[5] *Ibid* at 43, see art 17.
[6] EC, *Regulation 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] OJ, L 281/31.
[7] *Ibid* at 42.
[8] *Supra* note 4 at 51.
[9] *Ibid*.
[10] *Ibid*.
[11] *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, ECLI:EU:C:2014:317, [2014] ECR I-00000.

removal of the original publication of information from the Internet. Instead, it limits the removal of the personal information to the search result listed through search engine providers.[12] Therefore, while a search engine that has responded to a request under the *Regulation* will yield no relevant results, the 'erased' personal information will remain on the Internet, hiding in plain sight. This thesis will highlight, how, as a result of limitations such as this one, the *Regulation* can be a partial solution to the need for privacy protection only.

The recent case of *Google Spain*[13] decided by the Court of Justice of the European Union (*CJEU*) provides helpful insight into future application of the *Regulation*. The decision in *Google Spain* 'opened the floodgates' for the right to be forgotten, confirming that the right existed under the *1995 Regulation*.[14] The *CJEU* also confirmed that search engine operators must assume the role of the judiciary when faced with a request to remove personal information.[15] This thesis will demonstrate that placing such responsibility in the hands of private business is dangerous. While a movement away from the courtroom is becoming increasingly necessary as the Internet and aggrieved individuals grow, such a movement must be done with careful guidance. The EU has fallen short of this and provides little guidance relative to the impact the *Regulation* has on the Internet. While the EU touts the right to be forgotten as a win for the individual,[16] the cost to the Internet is immeasurable.

---

[12] *Ibid* at para 65.
[13] *Ibid*.
[14] *Ibid* at para 22.
[15] *Ibid*.
[16] EC, *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age*, (Munich: EC, 2012).

In examining the *Regulation* against the current legal climate of the Internet, this thesis will compare the protection it offers with the legal protections presently available in Canada and New Zealand. As part of that comparison, the effects of omitting a reasonable expectation of privacy from the *Regulation* will be discussed. The examination of these jurisdiction will highlight the huge step that Article 17 (the empowering provision of the right to be forgotten) takes towards providing broader privacy protection than is currently offered in Canada and New Zealand. Here, this thesis will lay the foundations for how the omission of a reasonable expectation of privacy severely impacts Article 17's effectiveness. In doing so, the importance of privacy will be discussed.

Although individuals can easily identify what they believe privacy is, legal debate continues as to how best to define privacy. Highlighting this discourse—the continual privacy debate—provides context for the right to be forgotten and the value that individuals and society place on privacy. As with all human rights, the importance of privacy on the Internet must be balanced against competing rights. Fortunately, courts are practiced in balancing privacy with other protected rights such as freedom of expression and freedom of information. Achieving an appropriate balance can allow for both the protection of the individual and the maintenance of the greater good to society. While this balancing act does not present a new assessment for the courts, the right to be forgotten shifts this exercise into new territory.

The Internet has gained praise for its accessibility and openness.[17] Its open architecture and freedom contribute to its success. Without such attributes, the Internet would not be accessible by over 3 billion users,[18] all able to contribute to an Internet that has gained popularity because of its openness and accessibility. Using *Google Spain* as an example, this thesis will examine the pressure the *Regulation* places on attributes such as openness and freedom of expression, arguing that such restrictions will stifle the Internet. It will argue that the *Regulation*, as interpreted by the EU, will negatively affect freedom of expression on the Internet. The current drafting of the *Regulation* impacts freedom of expression by casting an extremely wide net found in the omission of a reasonable expectation of privacy threshold common in privacy jurisprudence. Without this threshold, Article 17 permits any personal information to come within its crosshair. Not only has the EU cast a wide net in relation to accessing the right to be forgotten, it casts a wide net in its attempt to enforce Article 17 worldwide and further impacts freedom of expression across divergent jurisdictions. Finally, allowing private business to be both adjudicator and administrator where freedom of expression is concerned is a dangerous combination that, as this thesis will argue, will restrict freedom of expression as search engine operators are not properly equipped to play administrator and adjudicator. The *Regulation* enters dangerous territory where ill-equipped private businesses must determine whether certain personal information receives protection from freedom of expression or is simply deleted from

---

[17] Thomas Schultz, "Carving up the Internet" (2008) 19:4 European J Intl L 799.
[18] "Internet Usage Statistics: The Big Picture", (30 November 2015), *Internet World Stats* (website) online: <http://www.internetworldstats.com/stats.htm>.

the Internet. Drawing on examples such as the 'Great Chinese Firewall'[19] this thesis will illustrate what the Internet could look like under the *Regulation*.

Further, this thesis will argue that the *Regulation* is untenable in the climate the Internet currently operates within. The *Regulation* challenges traditional concepts of jurisdiction in an attempt to be as effective as possible. Establishing jurisdiction over the Internet is difficult as, unlike traditional concepts of jurisdiction,[20] the Internet transcends a state or national sovereignty. While the EU proposes that the *Regulation* should be applied globally,[21] this thesis will argue that in its current form such application is unattainable and only further infringes upon freedom of expression. Global application of the *Regulation* not only offends freedom of expression, it also highlights a critical failure of legal remedies available within the Internet. Without universal adoption, enactment of the right to be forgotten by only some jurisdictions is futile. Circumvention through the Internet is straightforward; the protection offered by the *Regulation* can be eradicated by simply altering the top-level domain of the search engine's website. Universal adoption of the right to be forgotten may be found in the introduction of a co-regulatory approach within the *Regulation*. Under this approach, those affected by Article 17 would have input into any regulation and therefore become more likely to globally adopt the

---

[19] *See* Tierney Bensen, Patrick Henze & Geoff Farnsworth "The Great Chinese Firewall: A Safegaurd or Stop Sign?" (2006) 2:3 Journal of Information Privacy & Security 42 at 51.
[20] Michael L Rustad & Thomas F Lambert Jr, *Global Internet law in a nutshell,* 2nd ed (Minneapolis: West Academic Publishing, 2013) at ch 3.
[21] EC, Commission, *Article 29 Data Protection Working Party 14/EN WP 225 "Guidelines on the Implementation of the Court of Justice of the European Union Judgment on 'Google Spain and Inc. V. Agencia Espanaola De Proteccion De Datos (AEPD) and Marios Costeja Gonzalez" C-131/12* (Brussels: EC, 2014) at 3.

amended *Regulation*. This thesis will argue that co-regulation provides the right to be forgotten with the teeth that Article 17 thought it had.

The *Regulation* has shifted responsibility from the judiciary to the private business. Search engine operators must both administer their own operations and adjudicate requests to remove personal information. They are incentivised to act quickly on such requests or face exorbitant fines.[22] In creating harsh penalties, the EU incentivises quick determinations - but at what cost? Shifting the balancing exercise required when assessing competing rights to private business is a dangerous move. Private businesses are not equipped to play both administrator and adjudicator. Comparatively, courts are well-versed at balancing subtle nuances in rights such as freedom of expression and personal privacy. This thesis will argue, that under the current drafting, private business will default to a tendency to remove information rather than truly act as an impartial adjudicator. Such arbitrary Internet censorship by private businesses leads to concerns for society and all individuals who are connected to the Internet. This shift, while increasingly necessary on the Internet as its penetration increases, must be exercised with caution and requires crucial buy-in from private businesses. Such buy-in from private businesses is essential in a borderless environment such as the Internet. This thesis will present a co-regulatory model that can alter behaviour of private businesses, be universally adopted and maintain protection for fundamental values such as freedom of expression and privacy.

---

[22] *Supra* note 4 at 92, see art 79.

Finally, this thesis will argue that not only is the Internet at risk of deteriorating under the right to be forgotten, so also is the protection of privacy. The risk to both comes as a result of shifting the focus from protecting privacy as a value to relying on the right to remove information from the Internet. Notably absent from the *Regulation* and Article 17 is the widely accepted privacy threshold of a reasonable expectation of privacy. This omission furthers the erosion of privacy as Article 17 does not align with how individuals use the Internet. In treating all information as private, the *Regulation* reduces the value of privacy. This thesis will argue that while certain personal information on the Internet must be protected by privacy not all personal information has a reasonable expectation of privacy. Further, this thesis will introduce a modified reasonable expectation of privacy test that considers social expectation of privacy. Protecting privacy is required to ensure that individuals have personal autonomy and emotional release and that society can grow and change without fear of ridicule or shame.[23] The *Regulation* is becoming the poster-boy for saving privacy on the Internet under the guise that all individuals will be empowered with control over their personal information. However, by moving our focus to the removal of information once it has been published and treating all personal information the same on the Internet we are firmly placing the ambulance at the bottom of the cliff.[24] That is, the right to be forgotten narrowly focusses on regulating search engines operators while ignoring the original publishers of personal information. Treating the symptoms and not the cause is a short-sighted and misconceived approach to protecting privacy. Privacy protection must look to the

---

[23] A F Westin, *Privacy and Freedom* (New York: Antheneum, 1967) at 32.

[24] The phrase "ambulance at the bottom of the cliff" refers to the act of solving a problem through treating the consequences rather than the cause of the problem. It is a restatement of the proverb "prevention is better than cure".

root cause and align with how individuals see privacy before it can appropriately be both accessed by individuals and assessed by private business.

1.1 Importance of Research

Protection of privacy in the context of the Internet has been a problem since the Internet's inception. The battle for control over the Internet and its data has been contemplated since decisions in early data transfer cases exposed how little the legal profession was equipped to manage the Internet.[25] Now, society's relationship with the Internet has reached an unprecedented level of connectedness. And this increased use of the Internet continues to exacerbate the tension between protecting privacy and protecting an open Internet. With over 3 billion users globally, the Internet has an impact on nearly half the population of earth. How governments and courts protect privacy must be reflective of how society values privacy. Legislative instruments, similar to the *Regulation*, do not reflect the value of privacy. Reactionary law-making is poor law-making, and often caters to the interests of the few.[26] Technology and the law, and in particular how technology is developed, will continue to impact society and more directly the legal profession. Ensuring that the game of 'catch-up' stops between technology and the law will come from directly addressing the cause, not the symptoms, of the problem. The *Regulation* is an update of the EU's previous directive on privacy on the

---

[25] *In re Lindqvist,* Case C-101/01, [2003] ECR I-12971 at I-13004.
[26] Emily Adams Shoor, *"*Narrowing the right to be forgotten: Why the European Union needs to amend the Proposed Date Protection Regulation*"* (2014) 39 Brook J Intl L 487 at 508.

Internet - the *1995 Regulation*.[27] If it is going to take another twenty years before the discussion of privacy and the Internet is tabled again, choosing the right answer is acutely important.

Over-reaching legislation,[28] like the *Regulation*, conjures up immediate fears for freedoms of expression and information and the role of censorship in society.[29] Two equally important notions that may be usurped if the legal profession and community accept the 'ambulance at the bottom of the cliff' as our panacea. Not only does the *Regulation* impinge on other rights, it shifts the balance of control further away from the individual, somewhat contrarily to its purpose. Such a shift is dangerous in the practice of law, and in particularly where the development of technology is in a perpetual flux.[30]

The further study of alternatives to the current theories of privacy on the Internet will lead to greater understanding of how the law should develop and be interpreted. It may also lead to more understanding in the public arena around how individuals can interact with law, technology and privacy.

---

[27] *Ibid*.
[28] Napoleon Xanthoulis "The right to oblivion in the information age: a human-rights based approach" (2013) 10 China Business Rev 84 at 91.
[29] *Supra* note 26 at 511.
[30] Alexander Tsesis, "The right to erasure: privacy, data brokers, and the indefinite retention of Data" (2014) 49 Wake Forest L Rev 433 at 482.

1.2 Structure of Thesis

This thesis is separated into 7 chapters. It begins with Chapter 1 exploring the right to be forgotten and the resulting restrictions the right will have on important legal values and concepts.

Chapter 2 will set the context for the protection of privacy on the Internet. It will discuss the current legal theory of privacy and why both individuals and society value privacy as a right. This discussion will demonstrate the continued need for protection of privacy as a central value, rather than as an afterthought. It will also outline how the current use of the Internet threatens the protection of privacy for individuals and has outgrown current regulation that has not caught up with the rise of technology. In outlining the current legal theory, the Chapter will address why privacy must be protected on the Internet.

Chapter 3 will introduce the right to be forgotten and consider the mechanics of the right in light of the recent *CJEU* decision in *Google Spain* and the *Regulation*. The Chapter will outline how an individual may request the removal of personal information from a search result. It will also look at three different scenarios the right to be forgotten aims to prevent. These scenarios will begin to highlight the caution that must be adopted in applying the right to be forgotten. The Chapter will suggest that the right to be forgotten clashes with traditional legal values of freedoms of expression and information, jurisdiction and Internet censorship, and will result in a decay in the value of privacy.

Chapter 4 will outline current protection available in relation to unauthorised disclosures of personal information in the jurisdictions of New Zealand, British Columbia, Ontario and Quebec.

This Chapter will compare the protection afforded by each jurisdiction to that offered by the right to be forgotten. These jurisdictions have been chosen to enable further contemplation on how the right to be forgotten significantly goes beyond what current remedies are available in these jurisdictions. This comparison will also highlight that a reasonable expectation of privacy is notably absent from the *Regulation*.

Chapter 5 comprises an in-depth critique of the right to be forgotten by outlining 3 perceived problems found in the right to be forgotten and its adoption: censorship, failure to consider the root cause and jurisdiction. This Chapter will outline how the right to be forgotten creates a real risk of unwarranted censorship on the Internet. Using examples of current censorship in play throughout the globe, this Chapter will argue that the right to be forgotten will foster more censorship and reduce the democratic force of the Internet. Here, the Chapter will outline that Article 17 can create a censored Internet despite only affecting search engine operators. This Chapter will argue that search engine operators who have been left with little guidance and faced with time and financial pressure may make flawed decisions that affect freedom of expression on the Internet. The *Regulation* risks devaluing privacy as it shifts away from a focus on what privacy represents to individuals to the wholesale deletion of content from the Internet. In relation to jurisdiction, the Chapter will highlight that without universal agreement across all jurisdictions, the right to be forgotten is severely weakened. While outlining that universal adoption of the right to be forgotten is unrealistic in its current form, this Chapter will examine how jurisdiction is typically established within a sovereign territory. The Chapter will conclude with a discussion on the current unsettled law in Canada in relation to establishing jurisdiction on the Internet.

Chapter 6 will offer alternative solutions to the *Regulation*. In doing so, the Chapter argues that the right to be forgotten continues to achieve its purpose of providing individuals with control over their personal information and reducing the wide net cast by the *Regulation*. The Chapter will offer solutions that better protect privacy by restricting access to the *Regulation* and refining internal procedures—through corporate social responsibility policy—undertaken by search engine operators.

Chapter 7 will provide a conclusion to this thesis. Here, the conclusion will summarize the arguments advanced in this thesis and reiterate the need for an amendment to the *Regulation* and Article 17. Such amendments will shift the right to be forgotten from being a partial solution only to an appropriate solution for the challenges privacy faces within the digital environment.

Chapter 2: The Importance of Privacy in General

Chapter 2 introduces the value of privacy. It will outline key theories of why society and individuals value privacy. This Chapter first introduces a workable definition of privacy that will be used in this thesis. Following on from the definition of privacy representing the control of personal information, it will introduce 4 theories that demonstrate why individuals and society not only value privacy but require it for survival. Within this context, this Chapter will discuss the importance of privacy in a digital environment. Focussing on how the new and dynamic Internet has bought about new privacy intrusions that require equally new legal remedies. This Chapter will conclude with a discussion of the permanence of digital memory and how it has altered the context of personal information on the Internet.

2.1 Valuing Privacy

In order to discuss privacy in relation to the Internet and the *Regulation* it is important to discuss first the differing definitions of privacy and consider why society values privacy. This section will set out three understandings of why individuals and society value privacy and discuss how such concepts materialise in society. Following that, and as a response to critiques, this Chapter will evaluate the need for privacy as a core human right.

2.1.1 Defining Privacy

> 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.[31]

While the definition of "privacy" in the *Oxford English Dictionary* provides an answer to what many individuals may view privacy as, the definition can only be a starting point for further examination. Importantly, the definition indicates that privacy manifests itself in different permutations. The many elements to privacy can be found in a single definition: it comprises a state or condition, being undisturbed or free, having a choice or right, and seclusion or freedom. It is here an examination of privacy can begin, with the understanding that this definition is a starting point only.

> Few values so fundamental to society as privacy have been left so undefined in social theory or have been subject to such vague and confused writing by social scientists.[32]

This quotation provides a good inroad into an examination of privacy and its definition. Privacy is somewhat of an enigma in modern academic literature as few fundamental values suffer from as much disagreement and confused theories. Although one may profess to know what privacy means to them, it is difficult to define as each culture and subculture will have its own

---

[31] *The Oxford English Dictionary*, 3rd ed, *sub verbo* "privacy".
[32] *Supra* note 23 at 7.

interpretation of what privacy means.[33] Privacy takes many forms and has vastly different meanings to individuals as they interact with society: Compare Western urban society, where families live in siloed housing separated from other families to that of the Java culture of the remote provinces of Indonesia, where families live as a community with not only shared housing, but also shared responsibilities such as child rearing.[34] For each culture privacy will mean something very different. A mother's physical intrusion into her teenage child's bedroom might be considered an unacceptable invasion of privacy in Western society but unremarkable in Java culture.

Privacy has been defined in countless ways since Warren and Brandeis coined it as "the right to be let alone" in there article published in 1890.[35] The article's genesis was the changing behaviour in print reporting and advances in technology. It set the foundations for ongoing academic discussion of what privacy is. William Prosser later split out the "jigsaw puzzle"[36] of privacy into four separate torts: intrusion, public disclosure, publicity and appropriation.[37] Alan Westin holds privacy to be related to the concept of information control and defined it 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.[38]

---

[33] Adam Moore, *Privacy Rights: Moral and Legal Foundations* (United States of America: The Pennsylvania State University Press, 2010) at 11.
[34] *Ibid* at 49.
[35] *Supra* note 1.
[36] William Prosser, "Privacy", Cal L Rev 48:3 (1960) 383 at 389.
[37] *Ibid*.
[38] *Supra* note 23 at 7.

Judith Wagner DeCew believes privacy represents information that is not generally a legitimate concern of others.[39] Together with the complex definition of privacy that appears in the *Oxford English Dictionary*, academic discourse illustrates the differing concepts of privacy that contribute to our understanding of privacy.

While the debate between the reductionist theories of privacy explored by academics such as Judith Jarvis Thomson and the coherentist theory famously discussed by Warren and Brandeis are acknowledged in this thesis,[40] they will not be explored. Rather, extracting from the differing theories and interpretations of privacy, this thesis proposes that control over oneself is central to the idea of privacy.[41] Control is crucial as new technology, such as the Internet—and the law that regulates it—advances and challenges who controls one's privacy. A right to privacy—on the Internet—can be seen as control over personal information (where it attracts a reasonable expectation of privacy) and a right to limit access to that information or at the very least control that access.[42] Privacy also includes a right of secrecy in relation to an individual's physical body and its location. Physical body and location privacy will not be the focus of this thesis but will represent peripheral elements of privacy discussed in this thesis.

---

[39] Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics, and the rise of Technology* (Ithaca: Cornell University Press, 1997) at 58.
[40] Stephen Penk & Rosemary Tobin (eds), *Privacy Law in New Zealand* (Wellington: Brookers, 2010).
[41] *Supra* note 33 at 25.
[42] *Ibid*.

Societies and individuals may inherently value privacy, but little is obvious as to why it is valued. The following section will introduce and discuss three theories on the value of privacy.

2.1.2 Personal Autonomy

Personal autonomy represents the ability to act alone, away from critique or comment: the ability to reflect, rebuild and question oneself. It is here that we find many of the answers to the question: what will we lose without privacy?

The belief that all individuals are free agents, and in this sense unique, is widely valued by democratic society. Society values the individual and the individual's ability to choose a path in life that they wishe to pursue. This premise relies on the presence of autonomy, the ability for an individual to—alone—discover themselves, who they wish to be and how they wish to think. The inner thoughts of a person can be depicted as their core-self that demands the ultimate protection of privacy.[43] The core of privacy must be protected to respect individuality and to prevent others from discovering (by foul means or fair) one's inner thoughts. It is this, an individual's inner thoughts, that allow them to grow and discover within society who they wish to be. It is also here, that the distinction between how an individual chooses to reveal herself in public and how they may act in private is revealed. This distinction is important as it allows individuals to develop into exactly that: an individual. If we were to take away the privacy of an individual's deepest thoughts, it is unlikely that these would materialize as social pressure tempers ideas outside of the norm. Thus, the protection of personal autonomy facilitates

[43] Beate Rössler, *The Value of Privacy* (Cambridge: Polity Press, 2005) at ch 3.5.

heterogeneous thought. Without this protection, individuals are open to scrutiny and social pressure to conform resulting in uniformity of thought. This was demonstrated in George Orwell's famous novel *1984* by the notion of Newspeak, a language adopted to control the thought of the citizens of the fictional totalitarian society named Oceania.[44]

If privacy is viewed as a residual concept, what is left when the individual is removed from the public gaze or out of earshot - then autonomy emerges. Individuals value a private zone and the ability to speak or think freely without others overhearing or disturbing their thought. Society can value individuality because, to varying degrees, it represents autonomy or the ability to go about life how one wishes.[45] It is at this juncture, between oneself in public and oneself in private, that the concept of differing personalities or the 'true' individual can emerge. This emergence of the individual qua individual is possible because privacy is a means of control. The ability to control the protection of privacy through autonomy allows an individual to decide what personal information is shared and with whom.[46] Developing autonomous relationships across a wide range of people is necessary in one's day-to-day interactions with others. For example, there is no reason for passengers of a bus to share the same level of personal information with their daily bus driver as they do with their siblings. The autonomy to regulate what personal information is shared allows the passenger to protect their private selves and prevent public intrusion.

---

[44] George Orwell, *1984* (New York: Plume, 1949).
[45] *Supra* note 43 at ch 3.5.
[46] *Ibid*.

2.1.3 Emotional Release

Emotional release is the expression of one's thoughts and feelings that, because of the pressure and expectations of society, are kept private to a certain extent.[47] Compared to the value placed on personal autonomy, being able to discuss with a close friend or partner what is on one's mind represents an outer layer of privacy. Taking the metaphor of an onion, as one peels back the outer shell (the outer, public mask) one reaches the centre, representing the individual's private core. The extension to different layers is made to trusted persons and to intimates.

As an individual fulfils various roles in society (for example, the university student, the sibling, the part-time employee) she faces varying expectations. The expectations faced daily create multiple personalities dependent on what is expected (a person might be unwise to express the same opinions to an employer as to a sibling). Throughout history people have performed different roles within society. Indeed, the original etymological meaning of person is mask.[48] The idea that a person 'masks' one's true self from the public has received criticism for being hypocritical.[49] While this criticism may be warranted in so far as a person effectively presents two personalities, such behaviour might equally be seen as a necessity. Privacy protection is not a one-way street. It is important to consider it in regard to the general public, or those who are being exposed to a person's private sphere (their inner onion layers).[50] Relief from the dual (or

[47] *Supra* note 23 at 32.
[48] *Ibid* at 34-35.
[49] *Supra* note 43 ch 7.2.
[50] *Ibid* at ch 3.4.

more) roles individuals 'play' results in the ability to be oneself in private. Without privacy, the façade would have to continue without any break.

2.1.4 Social Value of Privacy

So far the discussion has focussed on the protection of privacy from the individual's perspective. Although a valid point of view, it is not the only viewpoint. Privacy is commonly seen as the gate between the public and private spheres, between the collective and the individual.
The problem with framing privacy as an individual's concern is that this almost sets the individual up to fail. Because the territory that privacy treads is rife with opposing concepts and rights, conducting a balancing test that results in a favourable outcome for the individual can seem to be a rarity. If we take privacy as not only an individual value but also societal one, the balance becomes less fallacious.[51]

Indeed, privacy has social value. Personal autonomy and emotional release, although framed from an individual perspective, benefit society. The ability for an individual to escape the everyday pressures and expectations imposed by social norms allows for change in society:[52]

> Every intention, every improvement in art, technological, military, and political, has its genesis in the observation and ingenuity of a particular innovator. All utensils, traps, tools, weapons, stories, prove that someone exercised at some time initiative in deviating

[51] Daniel J. Solove *Understanding Privacy* (London, England: Harvard University Press, 2008) at 91.
[52] *Ibid* at 89.

> from customary models or standards. Accident played its part; but someone had to observe and utilise the accidental change before a new tool or custom emerged.[53]

In this way, the protection of the individual from constantly meeting social norms or expectations is of benefit to society. Such protection comes from shielding from the public an individual's lapse in social norms.[54]

Counter arguments cite that privacy makes social control vulnerable.[55] Modern society requires social control; it allows society to perform multiple functions without friction. This foible of privacy cannot be avoided and the idiom: 'A bad penny always turns up' is true in society. However, this fact cannot justify too little privacy. If the pendulum swings too much toward social control, society trades democracy for authoritarianism. The creation of modern-day blackmail laws in the eighteenth century saw privacy protect immoral behaviour.[56] Blackmail protection was created to protect those who were being subject to extortion.[57] In many cases the alleged acts were sodomy or adultery.[58] Thus the existence of blackmail pushed socially disapproved behaviour underground and instead of reprimanding the 'victim' society blamed the blackmailer as a scapegoat.[59] Such protection offered by privacy can prolong already slow-changing social norms, as above ground or in public the problem is not acknowledged.[60] The

---

[53] *Ibid* at 92.
[54] *Ibid* at 93.
[55] *Ibid.*
[56] *Ibid.*
[57] *Ibid.*
[58] *Ibid.*
[59] *Ibid* at 96.
[60] *Ibid.*

obvious alternative of 'airing the dirty laundry' is equally problematic and can cause disproportionate distress to a few. Thus while privacy may harbour social skeletons for longer than needed, failing to protect privacy at all with rampant disclosure would see the end of the individual's private sphere.

As a result, protection of privacy involves not only the protection of the individual's private sphere, but also protecting departures from social norms for all individuals. It is impossible for an individual to live in isolation. Social interaction is needed, as will be discussed in the pages that follow. Any relationship that individuals have is two-way; both parties must fulfil a social contract. Privacy should reflect this – it should be viewed not only in its immediate context but also in the greater picture, the social context.[61]

2.1.4.1 Privacy as a Requirement for Human Survival

The above discussion of the value of privacy can easily be criticised for being too subjective. An individual might argue, for example, that personal autonomy has little value in their life and this may be true. This criticism becomes stronger if we set this premise in the remote Java culture. However, subjectivity alone cannot be seen as sufficient evidence to discredit the value of privacy altogether. In response to such a claim, and without taking away from the aforementioned importance of the individual and social values, privacy can be better valued as an essential part of human flourishing.

---

[61] *Ibid* at ch 4.

To understand the need individuals have for privacy, we must first accept an individual's need for seclusion and separation. In doing so, the path becomes lit showing the evolution from seclusion to control over oneself with a focus on personal information. Alan Westin suggests that a human's need for privacy may be found in the animal world.[62] He illustrates this by explaining that many animals display their desire for seclusion through the act of establishing their territory.[63] Animals require their own territory to ensure the survival of their species, as without a private space to breed and nest, many animals will not survive beyond one generation. If an animal cannot lay claim to its own territory due to overpopulation, their survival is jeopardized as the flow-on effects from limited space impact on breeding, social interaction and sense of smell.[64]

Worryingly, overpopulation may lead to animals killing each other or "biochemical die-off".[65] A study of a population of 150 rats roaming freely in a cage saw in-fighting increase as the population increased.[66] Eventually the fighting became so widespread that rearing of the young rats deteriorated to a level where many did not survive. When the same sized cage was altered to include privacy enhancements a population of 5,000 was able to be supported.[67] Assuming that human evolution took place from the animal world, it is not too implausible to see the link with the animal kingdom's need for privacy to the same need being essential in human society.

---

[62] *Supra* note 23 at 8.
[63] *Ibid*.
[64] *Supra* note 33 at 47.
[65] *Ibid*.
[66] *Supra* note 33 at 48.
[67] *Ibid*.

Privacy for humans, who are inherently social creatures, provides the opportunity for disassociation. If humans did not have the ability to be free from one another there would be little stability in our social interactions. One can observe this phenomenon in the physical world: most modern houses have fences between neighbours, toilets typically have cubicles around them, and most windows are furnished with curtains or blinds. The ability to remove oneself from society provides one with control over access and behaviour exhibited when interacting with certain people. Individuals place such barriers between themselves and the rest of society to regulate behaviour and to enable self-definition of character. A helpful way to view the trajectory of privacy is over the life of an individual. A first-born has no privacy as they are totally reliant on their parent for full-time care. As the child grows older, he begins to request more privacy. For example, not wanting assistance to use the toilet. And as the child becomes an adult, he establishes privacy boundaries that are necessary for interaction with the outside world. These boundaries of association and chosen disassociation form the building blocks of relationships.

Robert Gerstein states:

> …there is a great difference between the way we experience our own action when we intend them to be observed by others and the way we relate to them when we are immersed in intimacy.[68]

[68] *Ibid* at 55.

His words provide a summary of the importance of privacy. Without privacy one may be unable to flourish as an individual. It is important to note that while presenting a case for the importance of privacy to everyone, privacy will not look the same to all individuals. However, while privacy is culturally diverse and subjective, the inability to control access to oneself and one's personal information may have universal negative effects on an individual's and society's well-being. Such negative effects are typically amplified by the widespread dissemination made possible through the Internet. Because of this added pain that the Internet can cause, protecting privacy on the Internet has become increasingly important in modern society.

2.2 Privacy in an Online World

In 2002, the 'Star Wars Kid' shot to global recognition after a video he produced was uploaded to the Internet, without his permission, resulting in the video going viral.[69] Although the Star Wars Kid has a name, for the millions[70] of people who have watched the video he is simply known as the Star Wars Kid. In the video the Star Wars Kid pretends to hold a light-saber and re-enact a scene from the popular movie franchise Star Wars. This is one of countless examples where the new world of the Internet rears its ugly head. While we tout the Internet as being an amazing tool for its connectedness, openness and ease of dissemination, it is exactly these characteristics that can lead to privacy intrusions and the unauthorized sharing of personal information.[71] With the Internet, you do not need to be well-known to have an audience.

---

[69] Saul Levmore & Martha C. Nussbaum (eds), *The Offensive Internet: Speech, privacy and reputation* (Cambridge: Harvard University Press, 2010) at ch 1.
[70] Jim Love, "Star Wars Kid" (January 15, 2006), online: YouTube < https://www.youtube.com/watch?v=HPPj6viIBmU > (At the date of this thesis, the video has over 30 million views).
[71] *Supra* note 69 at ch 1.

The way we live our lives has changed dramatically as a direct result of the advent of the Internet.[72] The Internet has made business more effective, communication virtually costless and the world a much smaller place. As uses for the Internet expanded, the name 'Web 2.0' was born.[73] Users of the Internet—and in particular users of Web 2.0—demonstrate an over-zealous concern with the digitization of the real world.[74] Such concern sees individuals upload, record, archive, publish, tweet, re-tweet, and share their experiences in real-time, further aided by the growth in Western and Eastern societies of ubiquitous mobile culture.[75] The activities undertaken by individuals participating in the Web 2.0 world have produced an environment where personal information has become a currency on the Internet.[76] The Internet is no longer used simply to find an interesting fact or directions to a restaurant; users also rely on the Internet as a surrogate for physical communities. The rise of community-based Internet activity has largely been facilitated by Social Networking Websites (*SNWs*) that first appeared at the beginning of the last decade. The most widely used SNW is Facebook, which was developed in 2004 and has had a meteoric rise in just over ten years of existence to now have over 1 billion users.[77] Somewhat expectedly, Facebook tops the list of removal requests under the *Regulation*

---

[72] *Dow Jones & Company v Gutnick,* [2002] HCA 56 at para 88.
[73] Chuck Lenatti, "Tim O'Reilly and Web 2.0" (2007) 7:22 The Seybold Report: Analyzing Publishing Technologies 13.
[74] A Ghezzi, A G Pereira & L Vesnic-Alujevic (eds), *The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten* (England: Palgrave Macmillan, 2014) at 54.
[75] *Ibid* at 53.
[76] Jef Ausloos, "The 'Right to be Forgotten' – Worth Remembering?", (2012) 28:2 Computer L & Security Rev 143 at 143.
[77] Facebook, Media Release, "One Billion People on Facebook" (4 October 2012), online: < http://newsroom.fb.com/news/2012/10/one-billion-people-on-facebook/>.

by Google.[78] The Internet has expanded its reach into the daily routine of the individual: it is now an accepted social norm to upload personal information to the Internet.[79]

The rise of both the use of and participation in the Internet is dumbfounding. With the ubiquitous use of the Internet, especially by the generation known as "Digital Natives",[80] the move of social practices from the physical world to the online world has an increased risk of privacy intrusions, like that of the Stars Wars Kid. In the pre-Internet world, the social practices of gossip and sharing information about one another were restricted to the local context, where such discussion took place. The Internet has changed this – the village is now global.[81] The problem with the "global village" is just that, the villagers are now global too. Without those on the receiving end of information having the right context, information is misused, mis-shared and misunderstood.

An immediate and obvious consequence of such widespread use of the Internet is the vast amount of information that is now available online. The vast information available on the Internet does not always lead to harm. In 2014 when Malaysian Airlines Flight MH370 went missing, "crowdsourced" scientists and mathematicians banded together in an attempt to

---

[78] Google, "European privacy requests for search removals" (24 July 2016), *Google Transparency Report* (website), online: <http://www.google.com/transparencyreport/removals/europeprivacy/?hl=en>.
[79] *Supra* note 74 at 1.
[80] Marc Pensky, "Digital Natives, Digital Immigrants Part 1" (2001) 9:5 On the Horizon 1 (Digital Native refers to a generation where computer technology and media-saturation have been the norm).
[81] *Supra* note 69 at ch 1.

calculate the missing aircraft's whereabouts.[82] In addition, much of the Arab Spring's[83] organizational success was a result of the Internet.[84] The democratization of access to the Internet enabled these global efforts to occur, as without it the cost of communicating and organizing en mass would be prohibitive. In spite of these positive outcomes, when we combine the attributes of the Internet; searchability, dissemination, anonymity and retained history, with the masses of personal information stored there, privacy concerns start to materialise.[85] The advent of powerful search engines such as Google—among others—only makes accessing information easier and faster. Today, if someone wants to find information about another person, the first inclination is to "Google" them.

2.3 The Digital Memory – A Gift or a Curse?

The use of the Internet is widespread. Not only has the Internet changed the way individuals interact with each other, its design has seen the corrosion of human memory.[86] One reason the Internet is heavily relied on by its users is that it does not forget.[87] Individuals do not need to employ their own memory when Google can do it more quickly and more accurately. Digital memory has the unique attribute—unlike human memory—of never forgetting. Because of the

---

[82] Chris Brown, "Flight MH370 gets crowdsourced help from scientists", *CBC News* (March 9 2015), online: < http://www.cbc.ca/news/technology/flight-mh370-search-gets-crowdsourced-help-from-scientists-1.2987450 >.
[83] The Arab Spring refers to the uprising in Egypt, Libya, Syria, Yemen, Bahrain, Saudi Arabia, and Jordan for democracy. Mobile technology using the Internet was used to not only to organize the democratic movement but also document the incumbent governments tactics.
[84] Habibul Haque Khondker, "Role of New Media in the Arab Spring" (2011) 8:5 Globalizations 675 at 677.
[85] *Supra* note 40 at ch 14.
[86] *Supra* note 74 at 84.
[87] Meg Leta Ambrose "It's About Time: Privacy, Information Life Cycles, and the Right to be Forgotten" (2013) 16 Stan Tech L Rev 369 at 388.

unprecedented level of connectedness individuals have with the Internet, there has been a shift resulting in the human default of forgetting and the digital default of remembering.[88]

Ease of access to the Internet furthers social reliance on the digital memory, ensuring that information is not forgotten. On the Internet the past and present are muddied as all information is presented in a flat order rather than chronologically. As information from the past remains available, an individual's present can be cluttered with their past.[89] The vast amounts of information available on the Internet, combined with the efficiency of search engines, also hinders an individual's ability to control their personal information.[90] The openness of the Internet is one of its defining characteristics, but paired with the current behaviour of its users, in particular, Digital Natives, there is a risk of it too becoming a curse. Individuals require space and distance away from society to think, recreate and develop themselves as the individual they choose to become. The Internet challenges this need and can make it nearly impossible for a person to "start over".[91]

Another shortfall with reliance on the Internet as a surrogate memory-bank is the deterioration of the original context in which personal information was uploaded. It is here, at the intersection between the search engines and digital memory, that intrusions of privacy can occur. Without

---

[88] *Supra* note 76 at 145.
[89] *Supra* note 74 at 84.
[90] *Supra* note 69.
[91] *Ibid*.

the original context, personal information available on the Internet can be used without reference to its original purpose and thereby inaccurately and possibly unfavourably.

The concept of privacy is a concept in flux that has lead to piecemeal regulation that has been unable to truly protect privacy in the age of the Internet. Individuals require control over their personal information to ensure that they can flourish as an individual and dare to go outside the norm without fear of critique. The space between society and the individual allows the individual to grow, discover and be autonomous. Providing an individual with control over their personal information not only benefits individuals but also society. As already discussed, society too benefits from privacy protection where individuals are able to think outside of social norms and create new ideas. Privacy allows for social interactions to occur without an individual losing total control of their self and allows individuals the right to choose how much and to whom they can reveal about themselves. The Internet challenges these concepts of privacy as not only is the social context now incomparably larger as the Internet continues to grow throughout the world, but unlike the human brain the Internet does not forget. Before the Internet, personal information was easier to control as individuals could only communicate in person (including by telephone) or through traditional publications such as letters, magazines or newspapers. These traditional communication methods represent communication where the individuals involved can be easily determined, making any form of redress simple. The Internet has both removed the social context of communication and the ability to identify who is the communicator. These two attributes added to widespread and easy dissemination make the Internet a perfect storm for a threat to privacy. Controlling personal information on the Internet is extremely difficult as while an individual might be aware of one offending website, there are good chances that there will be

countless more mirroring the offending personal information and breaching privacy. The threat posed to privacy by the Internet is not to be understated and the regulation to curb the current unrelenting privacy breach must also not be understated.

To open the discussion of how privacy must be regulated on the Internet, Chapter 3 will introduce and discuss the EUs current solution found in Article 17 of the *Regulation* and conclude with the argument that while the EU has not understated their attempt to regulate the Internet, it creates further problems for the Internet and must be amended.

Chapter 3: Introducing the Right to be Forgotten

This Chapter introduces the right to be forgotten as currently drafted in the *Regulation*. It outlines the mechanics and discusses three practical applications of Article 17. In doing so, the Chapter examines the relevance of Article 17 in light of these practical applications and questions whether Article 17 will be applied appropriately by search engines such as Google. This Chapter highlights the disparity between how Google and the EU see its application. In doing so, the Chapter discusses the abandonment of the judiciary in favour of an assessment undertaken by private businesses such as Google. The Chapter concludes with identifying 3 key problems that the right to be forgotten risks creating.

3.1 The Internet Records Everything and Forgets Nothing

The full name given to the regulation most famous for the coining the phrase "the right to be forgotten" is: *European Commission, Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulations)* (the *Regulation*).[92] The predecessor of the *Regulation* was passed into EU law in 1995. While it contains a host of updates to the current EU data protection policy, the *Regulation* has received the most attention, criticism, and discussion in relation the proposed right to be forgotten.[93] The *Regulation* was adopted by the European Parliament on 14 April

---

[92] *Supra* note 4.

[93] Recent Cases, "Internet Law – Protection of Personal Data – Court of Justice of the European Union Creates Presumption That Google Must Remove Links to Personal Data Upon Request – Case c-131/12, Google Spain SL v Agencia Espanola de Proteccion de Datos (May 13, 2014)" Harv L Rev 128 (2014) 735 at 738-739.

2016.[94] The adoption triggers a two-year transitional period where the EU's 28 member states must now incorporate the *Regulation* into their domestic legislation.[95]

The European Commissioner for Justice, Viviane Reding originally introduced the *Regulation* containing the right to be forgotten to the European Commission in January 2012.[96] Her introductory speech made the perceived importance of the *Regulation* clear: the EU will be at the forefront of privacy protection on the Internet and the right to be forgotten will provide a vehicle for doing so.

In her speech, Reding set a backdrop that was all too familiar – the Internet is a vast ever-changing and ubiquitous environment that individuals rely on more and more. In this context, Reding emphasised that individuals must be able to control their personal information and that the right to be forgotten will help to achieve this goal.[97] Reding boldly states: "I want to explicitly clarify that people shall have the right—and not only the 'possibility'—to withdraw their consent…"[98] The force and defiance of Reding's speech was indicative of the percevied need for a cure for the wide-scale pain felt by those who suffer a privacy intrusion on the Internet. However, while Reding displayed clear vision for the EU, the proposed cure must be approached with caution.

---

[94] EC, *Opinion 3/2015 (with addendum) Europe's big opportunity EDPS recommendation on the EU's options for data protection reform*, Opinion 3/2015.
[95] *Ibid* at 2.
[96] EC, *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age*, (Munich: EC, 2012).
[97] *Ibid*.
[98] *Ibid* at 5.

The right to be forgotten, while currently receiving attention, is not a novel concept. Its origins lie inside the EU, with Italy and France both having adopted a similar right, commonly known as the "right to oblivion". In France, the right permits convicted criminals to object to publications containing information about their convictions and imprisonment.[99] Other jurisdictions around the world have similarly adopted "clean slate" legislation, effectively wiping clean individuals' criminal records after a certain length of time has elapsed.[100] However, the Internet challenges the concept of 'wiping the slate clean' as it does not forget. While there is merit in the protection offered by Italy's and France's rights to oblivion, they are not adapted for a post-Internet world. The vast amount of content available online (both significant and trivial)[101] challenges the applicability of the right to oblivion, which was narrowly developed to conceal past criminal activity in limited circumstances. As Viviane Reding made explicit in her speech, there is an urgent problem relating to the preservation of information by the Internet; individuals now have extremely large digital shadows that will never be forgotten.[102] In allowing everyone to become an editor, journalist and publisher, the Internet has made everyone famous to 15 people.[103]

---

[99] Jeffrey Rosen, "The Right to be Forgotten", (2012) 64 Stan L Rev Online 88 at 88.
[100] *Criminal Records (Clean Slate) Act 2004* (NZ), 2004/36, s 7 (Section 7 provides that criminal conviction can be "clean slated" if the appropriate conditions are met).
[101] John Gantz & David Reinsel, "Extracting Value from Chaos" (June 2011), *IDC iView* (website), online: < https://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf > (In 2011 content generated from the Internet reached 1.8 zettabytes (a zettabyte is a million petabytes which is a million gigabytes)).
[102] *Supra* note 96 at 5.
[103] Jonatahn L Zittrain, *Future of the Internet and How to Stop It* (United States of America: Yale University Press, 2008) at 215.

The *Regulation* and the right to be forgotten attempt to alter the current trajectory of the availability of information on the Internet. Under the guise of giving individuals more control over their personal information, Article 17 of the *Regulation* states:

> The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:
>
> (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
>
> (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (1) of Article 9(2) and where there is no other legal ground for the processing of the data;
>
> (c) the data subject objects to the processing of personal data pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
>
> (d) the personal data have been unlawfully processed;
>
> (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society referred to in Article 8(1).[104]

Article 17 is the provision that has received most attention from privacy experts worldwide and provides the *Regulation* with its teeth. The Article provides individuals (data subjects[105]) the opportunity to make the Internet forget something about them. An individual has the right to request that information is removed if the information is "personal data" and on the applicable grounds.[106] The definition of "personal data" attempts to cast a very wide net and is defined as "any information relating to a data subject".[107]

The first trigger requires that the personal data is "no longer necessary for the purposes for which it was collected or otherwise processed".[108] This language is unhelpful as it requires an assessment as to whether retention of the personal data is 'necessary'. It also assumes that the personal data was necessary in the first instance: an assumption that, if untrue, undermines the *Regulation*.[109] The second trigger is withdrawal of consent by the individual. This avenue refers to Article 6 of the *Regulation*, which prescribes a framework for how personal data should be processed (with the individual's consent, to meet a contractual or legal obligation, to protect the individual and to ensure the performance of an act to be carried out in the public interest).[110]

---

[104] *Supra* note 4 at 43-44, see art 17.
[105] *Ibid* at 33, see art 4(1).
[106] *Ibid* at 43-44, see art 17.
[107] *Ibid* at 33, see art 4(1).
[108] *Ibid* at 43-44, see art 17.
[109] *Supra* note 101.
[110] *Supra* note 4 at 84 and 104.

Under the third avenue, the data controller must remove personal data if the individual objects to such data being processed in accordance with Article 6.[111] The individual may also object where the personal data is being used in marketing.[112] The final catch-all limb of Article 17 allows an individual to object where the processing of their personal data does not conform with the *Regulation*. While it is too early to gauge whether this trigger will be called upon often, it provides wider availability to the right than its alternatives.

Viviane Reding introduced the right to be forgotten to the EU as if it were to be entrenched, but noted that it will face the same balancing tests that other privacy protections offered by the courts must survive.[113] Reding stated "the right to be forgotten cannot amount to a right to the total erasure of history"[114], thereby stressing that any protection offered by the right will need to be balanced against other important rights such as free speech. This approach is inescapable. The courts have long been developing privacy as a right and/or value that must be balanced with other competing rights. Recognition of this fact also further tempers the teeth of Article 17.

3.2 The Right to be Forgotten – Practical Application

Before considering how the EU member states will apply Article 17, this section will further discuss how an individual can first access its protection. The three most likely scenarios that will

---

[111] *Ibid* at 104.
[112] *Ibid* at 106.
[113] *Supra* note 96 at 5.
[114] *Ibid*.

see the right to be forgotten invoked differ depending on how the personal data was uploaded to the Internet.

3.2.1 User Posted

The first possible scenario is where an individual uploads their own personal information to the Internet and subsequently wants it removed. This situation is likely to become more and more prevalent as digital natives mature and realize that content they previously uploaded to the Internet is no longer representative of them. This specific protection offered by the *Regulation* is quite unremarkable. While the *Regulation* gives legislative force to such protection, most SNWs currently allow individuals to remove their own content themselves. Although, while SNWs typically allow a user to remove their personal data from the public, they continue to store an individual's personal information for "as long as it is necessary"[115]

There is an obvious divide between an individual being able to delete content from their own site versus being able to delete it from the Internet entirely and Article 17 fails to address this anomaly. The right to be forgotten—in the case of successful requests—will delete content from the Internet, preventing both the individual who is concerned and everyone else from accessing such content. Deleting content from the Internet compared to deleting from a personal SNW page should not be treated as the same act. However, the right to be forgotten will treat all successful requests the same and remove the infringing content from the Internet. Under Article

[115] Facebook, "Facebook Data Policy – How can I manage or delete information about me" (30 January 2015), *Facebook* (website), online:< https://www.facebook.com/policy.php>.

17, this power shifts to private businesses who were not the original publishers and may have little vested interest in the relevant content. Further, and as will be discussed in Chapter 5, there are concerns that private businesses, such as Google, will not be suitable to assess whether content should be removed from the Internet where fundamental values such as privacy and freedom of expression are applicable.

3.2.2 Re-Posted

The second scenario involves personal data uploaded by an individual being 'shared' or copied and re-uploaded by another individual. Such behaviour is analogous to the Star Wars Kid discussed above. While the Star Wars Kid uploaded the video himself, the Internet and its connectedness allowed his personal data to be taken to an unintended and much wider audience. Assuming that his personal data meets the criteria in Article 17(1), the Star Wars Kid could invoke the right to request erasure of the re-uploaded personal data from search engine's results page. In the physical world, if such a sensation were to occur—for example the video was disseminated to a shop owner and proudly displayed in a shop window—the Star Wars Kid could easily locate that shop owner and request that they remove the copied or 'shared' content from public display. However, the Internet does not exist in a physical space, making it more difficult to locate and contact the sharers and "re-uploaders" of that personal data to request its removal.

The anonymity allowed by the Internet makes it easy to ignore such a request on the Internet as opposed to a person who walks in to a store after seeing copied content in the store window. Article 17 anticipates this challenge. After the uploader has either not responded or refused to remove the offending content, the harmed individual may request the relevant content provider

or host to remove the personal data. Assuming that the content provider or host meets the prescribed definition of "controller"[116] or "processor"[117], the personal data should then be removed. This scenario points to one of the key difficulties involved in applying the right to be forgotten. That is, application of the right causes a shift in responsibility from the judiciary to the private businesses. The problems associated with giving private businesses an adjudicative role are discussed in Chapters 5 and 6.

3.2.3 Third Party Posted

The final scenario removes the individual from the equation in so far as they are not responsible for uploading the personal data in the first instance. Here, the personal data is uploaded or shared wholly by a third party. As the Internet's grip on society expands, so too does the occurrence of personal data being uploaded without any involvement, or sometimes awareness, of the identifiable individual.[118] As this thesis will discuss below, traditionally privacy protection laws have responded to such violations via an intrusion tort or domestic legislation. However, neither of those models fit squarely with this scenario presented by a violation on the Internet. An intrusion tort is only made out where two key elements are present:

---

[116] *Supra* note 4 at 33, see art 4(7) (Controller is defined as "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law").
[117] *Ibid* at 33, see art 4(8) (Processor means "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.").
[118] *Supra* note 101 (The growth rate of the Internet increases at a rate of doubling every two years, it is expected in 2020 the digital world will be 44 times the size it was in 2009).

(a) a reasonable expectation of privacy; and

(b) publication of private facts that would cause embarrassment.[119]

The problem is two-fold. First, the courts are yet to accept whether the Internet is a public or private space.[120] Second, the requirement for publication to 'cause embarrassment' imports a subjective test that may not be easily met.

Having now introduced the instances where an individual can invoke the right to be forgotten as prescribed in the *Regulation*, this thesis will now look to how the EU member states will apply the right.

3.3 Google Spain and the Right to be Forgotten

As discussed above in Chapter 1, the right to be forgotten as introduced by the *Regulation* replaces its predecessor that was first introduced in 1995 (the *1995 Regulation*). The *Google Spain*[121] decision provides a useful case study of how the *Regulation* will be applied and interpreted when all 28 EU member states have adopted it into their domestic legislation. The CJEU, recognized that the right to be forgotten—as it is now commonly referred to—existed within the current *1995 Regulation*. The facts of the case, frequently traversed in academic literature,[122] will be briefly summarized for the purposes of this thesis.

---

[119] *Hosking v Runting,* [2004] NZCA 34, [2005] 1 NZLR 1.
[120] *Tucker v News Media Ownership Ltd,* [1986] 2 NZLR 716 (HC).
[121] *Supra* note 11.
[122] *Supra* note 93.

The case centred on a complaint lodged by Mario Costeja Gonzalez with the Spanish data protection agency (*AEPD*), a Spanish newspaper, and Google Spain. Mr. Gonzalez complained after becoming aware that a Google search of his name would return newspaper articles from 1998. The content of the newspaper articles related to a property formerly owned by Mr. Gonzalez and his former spouse being sold to repay social security debt. In the view of Mr. Gonzalez, the newspaper article was now irrelevant to his current life and therefore wanted the content removed from the Internet.[123]

The *AEPD* dismissed Mr. Gonzalez's complaint in relation to the Spanish newspaper but upheld the complaint that was directed at Google Spain. The *AEPD* distinguished the publication in the Spanish newspaper from the online publication as the newspaper publication was justified in accordance with Spanish law relating to the Ministry of Labour and Social Affairs.[124] The purpose of those relevant laws is to ensure the social security debt and property auction was provided with the maximum publicity to ensure a high number of bidders would attend the auction of the relevant property.[125] In coming to this decision, the *AEPD* stated that Google Spain was subject to the *1995 Regulation* and had to carry on its activities within the scope of that legislation.[126] Before making its decision, the Spanish Court decided to stay proceedings and refer the case to the *CJEU*.

---

[123] *Supra* note 11 at para 15.
[124] *Ibid* at para 16.
[125] *Ibid* at para 16.
[126] *Ibid* at para 17.

The focus for the *CJEU* was to interpret the 1995 *Regulation* and then apply it to the facts by determining whether:

a) Google Spain undertook any "processing of data";
b) Google Spain is a "controller";
c) Google Spain is subject to the territorial reach of the *1995 Regulation*; and
d) the "right to be forgotten" extended to search results displayed on the Internet.[127]

The *CJEU* found in the affirmative on all of the above questions and, in doing so, set the foundation for the right to be forgotten to enter into the mainstream. The *CJEU* easily established that Google Spain was processing data as it "collects", "retrieves", and "organizes" data.[128] Interestingly, Google Spain argued that it was not processing 'personal' data even though it processes data.[129] As Google's processing of data does not discriminate between personal and non-personal data, Google said it was not actively seeking to process personal data and therefore could not fall within the scope of the 1995 *Regulation*. However, this argument was rejected by the *CJEU*. The *CJEU* then found that Google Spain was a "controller" as it determined the purpose and means of its data processing.[130] In finding that Google Spain fell within the jurisdictional reach of the *1995 Regulation*, the *CJEU* established that while the data processing was not undertaken in Spain, the activities of Google Spain and its parent Google

[127] *Ibid* at para 20.
[128] *Ibid* at para at 28.
[129] *Ibid* at para 22.
[130] *Ibid* at para 38.

took place within the same context. For example, Google Spain, was responsible for advertising revenue within Spain. According to the *CJEU,* this made Google Spain an establishment of Google (the controller), therefore subjecting both to the *1995 Regulation*.[131]

Having determined that both Google and Google Spain were subject to the *1995 Regulation*, the *CJEU* then had to examine the extent to which they were subject to the right to be forgotten. In finding that the right to be forgotten was available to Mr. Gonzalez, the *CJEU* reiterated that a purpose of the 1995 *Regulation* is to ensure an individual's right to privacy.[132] The *CJEU* went on to stress that the protection of privacy is paramount in the EU as it is not only protected by the *1995 Regulation* but also the *Charter of Fundamental Rights of the EU*.[133] Interestingly, the same emphasis was not placed on the the competing value of freedom of expression, with the *CJEU* only briefly mentioning that a balancing exercise must take place in accordance with the *1995 Regulation*.[134] The *CJEU* directed that search results displaying the former social security debt of Mr. Gonzalez should be removed from Google Spain's results because the information was sensitive and the original publication took place in 1998.[135] It also noted that Google and Google Spain, as Internet search engines, were appropriate defendants as the originating website may not be subject to EU jurisdictions and its content could easily be re-published on a different website not known to the plaintiff.[136] Here, the *CJEU* acknowledges the almost universal use of search engines as a gateway to the Internet, but sets a dangerous precedent at odds with the

---

[131] *Ibid* at para at 55.
[132] *Ibid* at para at 66.
[133] *Ibid* at para 68-70.
[134] *Ibid* at para 74.
[135] *Ibid* at para 98.
[136] *Ibid* at para 84.

protection of privacy, by straying away from the deletion of information directly from offending websites.

The *Google Spain* decision gave the right to be forgotten the status of legal enforceability inside the EU. While the *CJEU* found that the *1995 Regulation* enshrined the right to be forgotten and that the right applied to Google, it should be noted that the *1995 Regulation* was introduced 3 years before Google existed and before the modern Internet was available to society. Nevertheless, the *CJEU* provided the footing for the right to be forgotten as an Internet norm. Since the widespread publication of the *CJEU's* decision,[137] Google has received 466,088 requests for removal of personal data from their search engine results.[138] From those requests, Google has only provided statistics on the top 10 websites that account for 8% of successful removal requests with a total of 63,062 URLs deleted from the Internet.[139] At just over an average of 2,300 request per day since the *CJEU's* decision, the perceived need for the right to be forgotten is obvious.

3.4 Applying the *Google Spain* Decision

It is important to note that the *CJEU* did not provide any guidance within its judgment as to how it should be applied.[140] Following the lack of direction from the *CJEU,* Google implemented a

---

[137] *Supra* note 93.
[138] *Supra* note 78.
[139] *Ibid*.
[140] *Supra* note 11.

system that received critique from the EU only six months after the ruling in *Google Spain*.[141] Under Google's system, an individual wishing to take advantage of the right to be forgotten must complete a form found on the Google website and simply wait while Google assesses the request. The EU has since attempted to provide more clarity around how to deal with right to be forgotten requests by issuing guidance rules.

3.4.1 Google's Approach to Right to be Forgotten Requests

Although Google is only one of many search engines that will be subject to the *Regulation* within the EU, its process will be used to describe how an individual may currently access the protection offered by the right to be forgotten in this section.

Fittingly, the entire process can be completed online. An individual wishing to have personal information removed from the results page on Google's search engine website begins by completing an online form. The form requires the following information to be completed:

a) the individual's full name;
b) a contact email address;
c) any URL the individual wants removed; and
d) an explanation as to why each URL should be removed.

[141] *Supra* note 21.

While the web form's simplistic requirements will be beneficial to individuals when completing a request, such simplicity is worrying when Google must assess competing interests of privacy and freedom of expression. After an individual has completed the form it is submitted to Google for their internal assessment. Little information is provided by Google as to how they will assess each submission. However, Google states it uses the following four steps to assess all submissions:

a) Does the request contain all the necessary information for Google to be able to make a decision?
b) Does the person making the request have a connection to a European country, such as residency or citizenship?
c) Do the pages appear in search results for the requester's name and does the requester's name appear on the page(s) requested for delisting?
d) Does the page requested for removal include information that is inadequate, irrelevant, no longer relevant, or excessive, based on the information that the requester provides? Is there a public interest in that information remaining available in search results generated by a search for the requester's name?[142]

Again, the simplicity of the assessment process is worrying as only one of the four steps actually considers legally relevant issues. As will be discussed in Chapters 5 and 6, private businesses

[142] *Supra* note 78.

are currently not fit to assess complex legal issues, which is evident by the overly simplistic process created by Google.

If the request is accepted by Google, the individual's name and the particular requested information will no longer appear in Google's search results in the relevant EU top-level domains.[143] Instead, the remainder of the organic search results will appear followed by a message from Google stating "Some results may have been removed under data protection law in Europe".[144] The simple process effectively makes the requested information invisible for all other users of Google's search tool within the EU. Importantly and interestingly, following the decision of *CJEU*, the information remains available and accessible on the Internet despite being invisible on Google's EU search engine websites.

3.4.2 EU Guidance to Right to be Forgotten Requests

Following the lack of guidance provided by the *CJEU*, the EU's Article 29 Data Protection Working Party (the *Working Party*), the expert advisor on EU data protection, published guidance on the *Google Spain* decision effectively providing Google and other search engine operators with rules on how to deal with right to be forgotten requests. Interestingly for Google, the *Working Party* clearly states that de-listing of specific links relating to the request should not be limited to top-level domains of the EU only.[145] The claim by the *Working Party* attempts to

---

[143] *Ibid*.
[144] Google Search, "Mario Gonzalez", *Google* (website), online: <https://www.google.es/#q=mario+gonzalez> (When completing a search for the name 'Mario Gonzalez' the following message appears: "Some results have been removed in accordance with the law of European data protection. More information").
[145] *Supra* note 21 at 3.

expand the jurisdictional reach of *Google Spain* while acknowledging the ease with which technology circumvents traditional legal rules. This is not the current practice for Google and despite the *Working Party's* paper being issued in November 2014, Google is yet to abide by such guidance.

Further, the *Working Party* discusses the scope of communication expected between the search engine providers, third party website hosts and users.[146] Effectively, the *Working Party* believes that communication should only occur between the user and the search engine operator as there is no legal basis under EU law or the *Google Spain* decision for any other parties to communicate. Although, there is no legal basis for such communication, common courtesy and prudent business practice should see communication take place, especially when considering the power that Google has to control traffic on the Internet. In addition, communication between users of the Internet and Google should be promoted. Removing content from the Internet creates gaps within what is believed to be an open system. Current Google practice is to communicate the removal of content.[147] To actively promote against this, the *Working Party* is creating a dangerous precedent and is heading down a slippery slope to an Internet dark-age.

Similar to the categories provided by Google[148], the *Working Party* sets out broad criteria that should be considered when assessing a request by an individual. Namely, the considerations are:

---

[146] *Ibid* at 10.
[147] *Supra* note 144.
[148] *Supra* note 78.

a) does the subject play a role in public life;

b) is the subject a minor;

c) is the data accurate;

d) is the data relevant and not excessive;

e) is the information sensitive;

f) is the information up-to-date;

g) is the subject put at risk;

h) the context of the publication; and

i) the legal context of the publication.[149]

In relation to paragraph (f) above, the *Working Party* states that out-of-date information will bear a presumption that it should be de-listed.[150] This 'shoot first ask questions later' approach again highlights the potential wide impact that de-listing information can have. This approach becomes increasingly discouraging upon the realization that the Internet has become societies' default archivist. While offering guidance is a step in the right direction, the *Working Party* should be cautious about providing presumptions that could lead to excessive use of the right to be forgotten. As already noted, search engine providers such as Google, are already ignoring aspects of the *Working Party's* guidance. Conflicting values are always competing in relation to the enforcement of a right and the situation is no different for the right to be forgotten.

---

[149] *Supra* note 21 at 13-20.
[150] *Ibid* at 18.

Certain elements of the *CJEU's* decision and the ensuing guidance by the *Working Party* are open to criticism: importantly the balancing that should take place between the protection of privacy and freedom of information. However, fault should not be passed to the *CJEU* but rather the drafting of the *1995 Regulation* and the *Regulation*, that places privacy as a paramount right above the others.[151] Ironically for Mr. Gonzalez, it would seem his pursuit for privacy secured his seat as a victim of the 'Streisand effect'[152] while paving the way for other individuals to request personal data be removed from search engines such as Google.

The result of this judgment can only be described as a watershed for the regulation of the Internet. If adopted outside the EU, it will have far-reaching consequences. Before providing an in-depth discussion of the limitations and restrictions that the right to be forgotten creates in Chapter 5, a brief overview of the problems of the continued application of Google Spain to the Regulation are as follows:

a) the high risk of increasing Internet censorship as private businesses are forced to take on an adjudicative role and the consequential chilling effect on freedom of expression;
b) devaluing privacy by treating the symptoms only; and
c) the worthiness (or lack thereof) of enforcing law that is easily circumvented by the grey jurisdiction of the Internet.

---

[151] Supra note 93 at 741.
[152] Guy Burgess, "Name suppression and the internet" (16 November 2009), *Law and technology* (blog), online: < http://www.burgess.co.nz/name-suppression-and-the-internet/> (In 2003 famous American singer, actress, and director Barbra Streisand set off an online phenomenon now know as the 'Streisand effect'. Ms Streisand attempted to have photographs of her sprawling Californian home censored from internet publication, only to have the opposite effect occur).

These problems will be discussed in greater detail and in light of the *Regulation* in Chapter 5.

Chapter 4: A Comparative Analysis: New Zealand, Canada and the Right to be Forgotten

This Chapter compares the current protection of privacy within New Zealand and the provinces of Quebec, Ontario and British Columbia in Canada with the protection offered by the right to be forgotten under the Regulation. It will highlight that the Regulation is boldly moving into new territory than what is currently available in the chosen jurisdictions. The ability to delete personal information from the Internet is not only a new remedy available in the toolkit for protecting privacy but also sees the judiciary replaced by private businesses. This Chapter contains a table to illustrate the different protection offered by different legal remedies throughout the chosen jurisdictions. It will conclude with a discussion on the notable absence of a reasonable expectation of privacy from the Regulation.

4.1 New Zealand

4.1.1 Common Law

The current status of privacy in New Zealand provides for interesting reading. Looking to the *New Zealand Bill of Rights Act 1990* (*BORA*),[153] that sets out fundamental rights and freedoms in New Zealand, privacy protection is notably absent. Although rights such as 'freedom of expression' and 'right not to be deprived of life' are present, a right to privacy is absent.[154]

[153] *New Zealand Bill of Rights Act 1990* (NZ), 1990/109.
[154] *Ibid,* ss 8 & 14.

There is no right to privacy present in the domestic legislation in New Zealand, instead one can find recognition of privacy as a right in the courts.

Justice Thomas in *Brooker v Police*[155] provides a detailed discussion recognising privacy as a right in New Zealand. *Brooker v Police* involved a protest outside a Police Constable's home in Wellington after Brooker believed he had been subject to unlawful police behaviour.[156] At the District Court, Brooker was charged with the offence of disorderly behaviour under section 4(1)(a) of the *Summary Offences Act*.[157] On appeal, the majority of the Supreme Court overturned Brooker's conviction finding his behaviour not to be disorderly and that the *Summary Offences Act* was not a sufficient restriction on the right to freedom of expression.[158] The Supreme Court states that the *Summary Offences Act* should be used to preserve public order rather than to protect the privacy of the Police Constable.[159] Thomas J cites numerous international covenants that recognize privacy as a right and in particular the *International Covenant on Civil and Political Rights* (*ICCPR*), Article 17.[160] The *ICCPR* is affirmed by the New Zealand Government in the long title of the *BORA*,[161] presenting a strong case for the right to be recognized by the courts. In *Brooker,* Justice McGrath, dissenting, discussed the reasons for not including privacy as a right in the BORA and concludes that its omission should not lead

---

[155] *Brooker v Police,* [2007] NZSC 30, [2007] 3 NZLR 91.
[156] *Ibid* at para 13.
[157] *Ibid* at para 17.
[158] *Ibid* at para 41.
[159] *Ibid.*
[160] *Ibid* at para 251 (Article 17(1) states "*No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation*.").
[161] *Supra* note 153.

to courts rejecting privacy as a right.[162] Thomas J concludes that above all, courts should look to the perception of privacy within society. Because society values privacy as a fundamental right the courts should provide certainty with regard to privacy. Privacy cannot be viewed as a fad but as something that is valued by all to enjoy.

While Thomas J's judgment in *Brooker v Police*[163] clearly sides with privacy as a right, there is still disharmony amongst the New Zealand judiciary as to the status of privacy. Justice Tipping in *Hosking v Runting* (*Hosking*) sees privacy as a value (or a collection of values) rather than a right. The facts concerned celebrity parents who objected to their children been photographed in a public street and the ensuing publication in a lifestyle magazine.[164] The Hoskings had taken part in several interviews about the pregnancy as their children were conceived with the use of IVF treatment.[165] Mr. Hosking, who was a television news presenter at the time, sought an injunction to prevent the publication of the photographs by the magazine.[166]

The general right to privacy, which was envisaged by the legislature prior to the enactment of the *BORA*, has never materialized. Despite this, privacy is protected in New Zealand, and recognized as a right when framed by the decision and facts of *Hosking*.[167] In that decision the Court of Appeal recognized that individuals have the right to be protected from unauthorized dissemination of private information. This should be seen as an in-road to more recognized

---

[162] *Supra* note 155 at para 122.
[163] *Supra* note 155.
[164] *Supra* note 119 at 9.
[165] *Ibid.*
[166] *Ibid* at 1.
[167] *Supra* note 119.

privacy protection, and in particular privacy protection that extends outside of the narrow framework outlined at common law.[168] New Zealand has not recognized a general privacy right in statute but still offers some protection in regard to privacy. The recognition of privacy is in the form of a tort created by a slim majority in the decision of *Hosking*.[169]

While the Court did not recognize that the facts were sufficient to warrant a remedy, the majority accepted that the tort of invasion of privacy existed in New Zealand.[170] The Court stated that tort required two elements to be satisfied in order for any privacy claim to be successful. Justice Gault and Justice Blanchard set out the elements of the tort as:

a) The existence of facts in respect of which there is a reasonable expectation of privacy; and
b) Publicity given to those private facts that would be considered highly offensive to an objective reasonable person. [171]

Blanchard and Gault JJ quickly recognised that these two elements were not exhaustive, and felt that the tort would be shaped by later courts.[172] Although an issue comparable to *Hosking*[173] has

---

[168] *Rogers v TVNZ,* [2007] NZSC 91 at para 23 (Chief Justice Elias comments (ambiguously) on *Hosking* and the length the courts have explored privacy in New Zealand).
[169] *Supra* note 199.
[170] *Ibid.*
[171] *Ibid* at para 209.
[172] See *C v Holland,* [2012] NZHC 2155, [2012] 3 NZLR 672 (Here the High Court developed a separate tort for an intrusion of privacy without the requirement for publication. Justice Whata commented that the new tort must remain consistent with the tort established in *Hosking*).
[173] *Supra* note 119 at para 209.

not reached the Supreme Court in New Zealand and thus the test is not set in stone, the affirmation by the Court of Appeal has provided a valuable starting point. It must be expected that any privacy case involving publication will come up against the *Hosking* test, which stands as the foundation for continuing privacy debate in New Zealand.

4.1.1.1 Common Law and the Right to be Forgotten

The common law protection in New Zealand is aligned with the end result of the right to be forgotten as both legal remedies attempt to curb unauthorized disclosure of personal information. However, the common law protection does not extend to the length that Article 17 does. While none of the cases discussed centre around the Internet, the remedies available at common law do not extend to a court making an order that personal information is deleted. Rather, courts in New Zealand will grant an injunction to prevent unwanted disclosure of personal information. An injunction prevents further disclosure but is not backward looking and therefore any previous publications will evade the remedy set out by a court in New Zealand. In comparison, Article 17, when triggered, will see personal information deleted as the default remedy. This comparison highlights the additional—and somewhat drastic—step the EU has taken with its introduction of the *Regulation*. Not only is the EU attempting to alter the past, but it is boldly moving where other jurisdictions are currently not while sidestepping the judiciary completely.

The protection offered at common law in New Zealand is more difficult to access than the right to be forgotten under the *Regulation*. To trigger the right to be forgotten an individual must only

prove that personal data—defined as "any information relation to a data subject"[174]—has been disclosed. Unlike the right to be forgotten, the common law protection required additional requirements to be met in relation to the personal information: the information attracts a reasonable expectation of privacy.[175] Such a requirement is absent from the right to be forgotten, allowing any information about a person to be subject to the right to be forgotten. The extremely wide net cast by the right to be forgotten not only will see a huge influx of requests but it also strays away from the protection of personal information that is private to any personal information. Courts have established the reasonable expectation of privacy threshold to limit their protection to personal information that individuals and society values as attracting privacy. As discussed in Chapter 2, privacy is a nebulous and subjective concept and the reasonable expectation of privacy assessment is a pragmatic solution to enable a line in the sand to be drawn.

Further, the common law tort in New Zealand requires that the publication be highly offensive to an objective reasonable person. The right to be forgotten requires no such assessment and presumably assumes that any publication that occurs on or through a search engine website is highly offensive. Similar to assessment undertaken when evaluating a reasonable expectation of privacy, the highly offensive assessment enables courts to evaluate the merits of an issue and decide whether the relevant personal information qualifies for a legal remedy. Without such

---

[174] *Supra* note 4 at 33, see art 4(1).
[175] *Supra* note 119 at para 209.

assessments courts would see a huge volume of claims relating to personal information where there is no real privacy concern.

While it cannot be said that the right to be forgotten does not have parameters that must be met—for example if the individual withdraws consent from the processing of their personal data—the threshold to access the right to be forgotten is significantly lower than the protection offered through the common law in New Zealand.

4.1.2 The Privacy Act 1993

The *Privacy Act 1993* (the *NZ Privacy Act*) outlines the legal framework for how personal information should be collected, used and disclosed with its 12 privacy principles.[176] The *NZ Privacy Act* regulates this behavior not only in relation to private businesses but also individuals who hold personal information about other individuals. Similar to the approach discussed below in Canada and her respective provinces, the *NZ Privacy Act* attempts to provide individuals with greater control over their personal information.

Principles 7, 8, 9 and 10[177] are relevant to this thesis as they regulate the correction, access, time-limits and disclosure of personal information within New Zealand. Principle 7 of the *NZ Privacy Act* relates to an individuals' ability to correct personal information held by an agency. Principle 8 states that an agency must ensure that information held about an individual is accurate, up to

[176] *Privacy Act 1993* (NZ), 1993/28, s 6.
[177] *Ibid*, s 6.

date, complete, relevant and not misleading. Principle 9 prevents an agency from retaining information for a time that is longer than necessary. And Principle 10 limits the use to which an agency may put the relevant personal information.

In comparison with a complaint that is bought to the courts under the tort of invasion of privacy, the Privacy Commissioner encourages that *NZ Privacy Act* complaints are resolved informally between the relevant parties. Failing this, individuals may bring a claim directly to the Privacy Commissioner.[178] In the event that a complaint is received by the Privacy Commissioner, it can either be investigated or the Privacy Commissioner has the right to take no action in relation to the complaint.[179] Under the *NZ Privacy Act*, there is no ability for the Privacy Commissioner to prosecute or fine individuals, rather the Privacy Commissioner seeks to settle disputes and educate compliance with the *NZ Privacy Act*.[180]

4.1.2.1 The *NZ Privacy Act* and the Right to be Forgotten

None of the above relevant principles from the *NZ Privacy Act* align with the right to be forgotten. Primarily what is absent from the *NZ Privacy Act* is the ability for an individual to have their information removed by an agency. Whether search engine operators such as Google would fall within the definition of "agency"[181] under the *NZ Privacy Act* is also a moot point as the definition does not align with "data controller"[182] found in the *Regulation*. The *NZ Privacy*

---

[178] *Ibid*, s 67.
[179] *Ibid*, s 70.
[180] Privacy Commissioner, "Frequently Asked Questions", *Privacy Commissioner* (website) online: <https://www.privacy.org.nz/your-rights/frequently-asked-questions/#fine>.
[181] *Supra* note 176, s 2(1).
[182] *Supra* note 4 at 33, see art 4(7).

Act and the right to be forgotten offer different tools for regaining control of an individual's personal information and therefore provide some legitimacy for adoption of a legislative right paralleling the right to be forgotten in New Zealand. However, as will be discussed in Chapter 5, the many problems of the right to be forgotten may override this legitimacy.

4.2 Canada

As there is no unified law protecting privacy in Canada, the protection of privacy in Canada is found in a number of places including: federal legislation, provincial legislation, common law doctrines and equitable principles. Due to the many variations in privacy protection across each province in Canada, this section of the thesis will discuss privacy protections offered in Quebec, Ontario and British Columbia only. These three provinces all protect privacy with varying approaches and thus provide a good demonstration of privacy protection within Canada.

Prior to the adoption of the intrusion upon seclusion tort in Ontario, the courts in Canada have protected intrusions of privacy through the application of already established torts or through the application piecemeal of privacy-esque legislation. The scope of this thesis does not require a discussion on each separate tort, instead a list of the available torts provides an illustration of the varied outcomes that may occur in court when attempting to protect one's privacy:

a) Trespass;
b) Nuisance;
c) Negligence;
d) Defamation and Injurious Falsehood;

e) Misappropriation of Personality; and

f) Breach of Confidence and Fiduciary Duty.[183]

The *Personal Information Protection and Electronic Documents Act*[184] (*PIPEDA*) and similar provincial statutes in British Columbia[185] and Quebec[186] also offer privacy protection to individuals in a form of control. The purpose of such legislation is to provide individuals with control over personal information held by private businesses.[187] The thesis, in the following sections, will outline the control afforded to individuals by each province.

4.2.1 Quebec

4.2.1.1 Civil Law

The Supreme Court of Canada, using the *Quebec Charter of Rights and Freedoms*[188] (the *Quebec Charter*), accepted that an invasion of privacy had occurred and could be remedied in the case of *Aubry v editions Vice-Versa Inc (Aubry)*[189].

The facts of *Aubry* are particularly interesting for this thesis as it involves the dissemination of a photograph in a public place. The majority of the Supreme Court held that the respondent's

---

[183] CED 4th (online), *Torts*, "Introduction" (I.1) at § 2.
[184] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.
[185] *Personal Information Protection Act*, SBC 2003, c 63.
[186] *An Act Respecting the Protection of Personal Information in the Private Sector*, CQLR 1993, c P-39.1.
[187] See *Personal Information Protection Act*, SBC 2003, c 63, ss 1-2, Personal Information Protection and Electronic Documents Act, SC 2000, c5.
[188] *Charter of Rights and Freedoms*, CQLR, c-12, s 5.
[189] *Aubry v Editions Vice-Versa Inc,* [1998] SCR 591, [1998] 1 RCS 591.

privacy had been infringed. The Court found that a privacy breach had occurred when the identifiable image was published without consent, unless it was justified by the public interest.[190] The Court relied on the *Quebec Charter* and in particular section 5: "Every person has a right to respect for his private life."[191] The majority drew out a right to one's image on the basis that section 5 protects individual autonomy:

> "If the purpose of the right to privacy guaranteed by s. 5 of the Quebec Charter is to protect a sphere of individual autonomy, that right must include the ability to control the use made of one's image, since the right to one's image is based on the idea of individual autonomy, that is, on the control each person has over his or her identity."[192]

The photo in question was taken for publication in an artistic magazine without the respondent's permission. The analysis by the majority states that if the photo had not focused on the respondent, the action would not have been successful.[193] The Court stated that this would be more analogous to a photo of a crowd at a sporting event, where no one in particular is the subject.[194] In addition the Court states that if a person could be identified but the picture clearly directs attention elsewhere, there can be no materialization of a privacy claim.[195]

---

[190] *Ibid* at 615.
[191] *Charter of Rights and Freedoms*, CQLR, c-12, s 5.
[192] *Supra* note 189 at para 15.
[193] *Ibid* at para 59.
[194] *Ibid* at para 21.
[195] *Ibid* at para 22.

The Court states that if the circumstances involve a public setting that is simply a background to the individual, the fact that the photo was taken in a public place becomes irrelevant.[196] This established protection for the plaintiff and set parameters for when privacy can be protected in a public setting.

It is important for this thesis that the Court discussed the effect a public place has on the expectation of privacy. The decision in *Aubry* is pragmatic as it does not allow the public setting context to be used to evade the protection of privacy.

4.2.1.1.1 Civil law and the Right to be Forgotten

Similar to the parameters of the right to be forgotten, the civil law approach in Quebec sets the bar low for what personal information can attract privacy protection. In *Aubry* the offending publication arose out of an identifiable photo of an individual in public taken without consent.[197] Contrasting this to the sentiment in New Zealand and in particular the facts of *Hosking*, such a photo would not attract privacy protection as there is no reasonable expectation of privacy.[198] Quebec civil law also aligns with the right to be forgotten in the balancing exercise it contemplates with public interest. Article 6.1(e) of the *Regulation* also stipulates that data processing will be lawful, despite the right to be forgotten, if such processing is in the public interest. As the facts in *Aubry* do not relate to publication on the Internet, it is difficult to draw

[196] *Ibid* at para 22.
[197] *Ibid* at para 1.
[198] *Supra* note 119 at para 164.

direct parallels. However, the focus of the Court's analysis was on the unauthorized publication of information about an identifiable individual. Such sentiment aligns closely with the purpose of the *Regulation* as spelled out by Viviane Reding when she introduced the *Regulation* into the EU Parliament.[199] However, evident in the comparative analysis with New Zealand, the *Regulation* goes beyond what civil law remedies are available in Quebec. In *Aubry*, the Court awarded damages as a result of the finding that the plaintiff's privacy had been infringed.[200] In comparison with the *Regulation*, while search engine operators may face penalties, there is no scope for an award of damages to the individual concerned. The finding that the plaintiff's privacy was intruded upon after the photo was published restricted the Court's ability to grant an injunction and prevent the publication. The *Regulation* does not include injunctive relief either. Here we see the remediation available in the *Regulation* going well beyond what Quebec currently offers.

4.2.1.2 *Quebec Private Sector Privacy Act*

Quebec has adopted its own *PIPEDA* in the form of *An Act Respecting the Protection of Personal Information in the Private Sector*[201] (the *Quebec Private Sector Privacy Act*) to provide individuals with control over their personal information when collected, used or disclosed by private businesses. Similar to the protection and availability of control provided in the federal *PIPEDA*, the *Quebec Private Sector Privacy Act* provides overarching principles to be maintained by enterprises (corporations):

---

[199] *Supra* note 96
[200] *Supra* note 189 at para 72.
[201] *Supra* note 186.

a) A person or enterprise must have a serious and legitimate reason for establishing a file on someone;[202]
b) Every individual has the right to access his or her file, unless the right of third parties must be protected or there is a serious reason for refusing access;[203]
c) Every individual has the right to rectify an incorrect, incomplete or obsolete file; and
d) Every person or enterprise that opens a file on an individual has an obligation of confidentiality.[204]

Although the *Quebec Private Sector Privacy Act* does not contain a definition of what an enterprise is, the courts have been willing to accept a wide range of organizations to be enterprises under the *Quebec Private Sector Private Act*.[205] Further, personal information has been defined broadly to include any information relating to a natural person in their capacity as an individual or information that identifies an individual.[206]

The *Quebec Private Sector Privacy Act* makes it the responsibility of the enterprise to ensure unauthorized disclosure does not occur.[207]

---

[202] *Ibid*, s 4.
[203] *Ibid*, s 8.
[204] *Ibid*, Division III ss10-17.
[205] Canada, Privacy Commissioner of Canada, *Learning from a Decade of Experience: Quebec's Private Sector Privacy Act*, (Ottawa, Privacy Commissioner of Canada, 2005) at 1.2.
[206] *Ibid* at 1.4.
[207] *Supra* note 186, s 13.

4.2.1.2.1 *Quebec Private Sector Privacy Act* and the Right to be Forgotten

The control in the *Quebec Private Sector Privacy Act* should be seen as attempting to achieve a similar goal to that of the right to be forgotten, shifting the balance of power from the large unknown (sometimes represented by enterprises or corporations) to the user or individual. In addition, the definition of personal information is the same as the definition found in the *Regulation.*[208] These similarities point toward an acceptance of the rationale behind the right to be forgotten but Quebec does not extend its reach as far as the *Regulation*. The *Quebec Private Sector Privacy Act,* similar to the *Privacy Act* in New Zealand, does not center the ability on an individual to have personal information removed by the enterprise. This additional step, found in the right to be forgotten, highlights the leap the right to be forgotten is making in comparison with current legislative protection. While this bold move is argued as necessary by the EU, it must be approached with caution and careful consideration before being invoked.

4.2.2 Ontario

4.2.2.1 Common Law

The Court of Appeal for Ontario recently incorporated the United States' intrusion tort as a protection of privacy called "an intrusion upon seclusion"[209]. While the earlier decision from the Ontario Supreme Court of Justice denied the existence of such a tort in *Jones v Tsige*[210], the Court of Appeal over-ruled it.[211]

---

[208] *Supra* note 4, at 33, see art 4.
[209] *Jones v Tsige,* 2012 ONCA 32 at para 19, 251 CRR (2d) 124.
[210] *Jones v Tsige,* 2011 ONSC 1475, 199 ACWS (3d) 1367.
[211] *Supra* note 209.

The facts of *Jones v Tsige* involved the unauthorized access of the appellant's banking records by the respondent.[212] The Court of Appeal in reviewing the earlier Supreme Court decision held that a right of action for intrusion upon seclusion should be recognized in Ontario.[213] In doing so, the Court recognized that substantial changes and development were constantly being made in the realm of technology and the Internet. The Court further explained that it was within its scope to establish such a tort and consequently quashed a common conception that privacy protection should be established through the legislature only.[214]

The Court adopted the elements that have been developed in the United States' *Restatement (Second) of Torts* (2010). The elements of the adopted tort are:

a) an intentional and unauthorized intrusion;
b) that intrusion was highly offensive to the reasonable person;
c) the matter intruded on was private; and
d) the intrusion caused anguish and suffering.[215]

Importantly, the Court noted that the established tort would not open the "floodgates" as it would have to be balanced against other competing values.[216] The Court concluded that the plaintiff

---

[212] *Supra* note 209 at para 4.
[213] *Ibid* at para 65.
[214] *Ibid* at para 68.
[215] *Ibid* at para 71.
[216] *Ibid* at para 73 (See the discussion in relation to the competing rights of freedom of expression and freedom of the press).

had suffered loss and awarded $35,000 to the plaintiff.[217] In doing so, the Court took a holistic assessment of the facts, among others; the nature of the wrongful act, the effects on the plaintiff's health, and any stress or annoyance caused by the defendant.[218]

4.2.2.1.1 Common Law and the Right to be Forgotten

Similar to the tort adopted in New Zealand, the Ontario Court of Appeal has created a number of limbs that must be met before the tort can be established. And similarly to the current protection offered by the common law in New Zealand, the right to be forgotten does not align with the tort created in Ontario. In particular, the second limb of the test requires that the intrusion was highly offensive to the reasonable person. Establishing a much higher threshold than the primary requirement under the right to be forgotten, where an individual can request removal of personal information because it is no longer necessary.[219] Without discussing the vague meaning of 'necessary' under the right to be forgotten, the threshold is much lower and provides for a significant number of individuals who will be able to access the right to be forgotten. The third limb in Ontario requires that the relevant personal information is private, while the Court did not define private information, it did refer to a number of Commonwealth cases, including *Hosking*, where a reasonable expectation of privacy was established.[220] Following these cases, it seems that Ontario courts will also require a reasonable expectation of privacy to exist before any protection can be offered. Such an assessment is absent from the right to be forgotten and

---

[217] *Ibid* at para 13.
[218] *Ibid* at para 87.
[219] *Supra* note 4 at 43, see art 17.
[220] *Supra* note 209 at para 64.

underscores the different thinking between the new privacy protection in the EU and the current understanding in Ontario.

Not only is the rationale different between the EU and Ontario, the remedies available also differ. While the facts in *Jones v Tsige* did not occur on the Internet, the Court discussed damages where no actual loss was evident or calculable. In awarding damages, absent of a publication, the Court took a comprehensive assessment of the facts. The *Regulation* does not contain an award for damages but rather incentives quick removal of the infringing publication with exorbitant fines. The teeth and remedy of Article 17 is the removal of the infringing content from the Internet by search engine operators. In comparison with an award of damages or an injunction, Article 17 takes the bold step of deleting the content. The step taken by the EU must be seen as bold in comparison with an injunction, which is typically issued by the relevant court and against a publisher. Under the *Regulation*, the deletion occurs without the input of a court and must be carried out by the search engine operator. While the end result of an injunction and deletion may appear to be aligned, deleting content from the Internet—without cautious consideration—can lead to further harm. Harm caused by Article 17 is discussed in detail in Chapter 5.

4.2.2.2 *PIPEDA*

Unlike the provinces of Quebec and British Columbia, Ontario has not adopted its own *PIPEDA*. Ontario adopted the *Personal Health Information Protection Act 2004*[221] in relation to health

[221] *Personal Health Information Protection Act*, SO 2004, c 3.

personal information only, leaving the remainder of *PIPEDA* applicable to the province of Ontario. As stated above, *PIPEDA* provides a foundation for the collection, use and disclosure of personal information by private businesses and is the genesis for the legislation now adopted in Quebec and British Columbia.

PIPEDA ensures that private businesses collect, use and disclose personal information within a framework that is lawful and with the relevant person's consent.[222] Schedule 1 to *PIPEDA* contains the full force of *PIPEDA* and sets out the basic privacy obligations that must be adhered to in relation to personal information.[223] For the purposes of this thesis, the relevant principles are:

a) An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.[224]
b) The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.[225]
c) The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.[226]

---

[222] *Personal Information Protection and Electronic Documents Act*, SC 2000, c5, s 3.
[223] *Ibid*, Schedule 1.
[224] *Ibid*, Schedule 1, Principle 1.
[225] *Ibid*, Schedule 1, Principle 3.
[226] *Ibid*, Schedule 1, Principle 4.

d) Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.[227]

e) Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.[228]

f) Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.[229]

Although the *PIPEDA* is limited to personal information held by a private business within the jurisdiction of Canada it offers individuals greater control over that information.

4.2.2.2.1 *PIPEDA* and the Right to be Forgotten

As already mentioned, such protection closely aligns with that of the proposed right to be forgotten. As individuals face greater access to technology and ease of which personal information can be shared, there is a greater need for control. However, principle (a) creates an interesting comparison with the right to be forgotten. Principle (a) requires that an organization that has personal information under its control becomes accountable for such information.

---

[227] *Ibid*, Schedule 1, Principle 5.
[228] *Ibid*, Schedule 1, Principle 6.
[229] *Ibid*, Schedule 1, Principle 9.

Although Google was found to be a "data controller" for purposes of the *Regulation*[230], it is not settled law and remains controversial. For the *PIPEDA* to apply to Google, the rationale that Google is in control of one's personal information when it displays search results through its search engine website would have to be followed. Principle (e) also creates an interesting comparison with the right to be forgotten. In stating that personal information cannot be disclosed for any other purpose than for which it was collected, principle (e) seemingly aligns with exactly the purpose of a search engine. A search engine indexes (read: collects) information on the Internet to be displayed when relevant search queries are entered. Such disclosure is only for the purpose of displaying results to the individual making the search request. Although Google was found to be a "data controller" for the purposes of the *Regulation*, it does not contain the same exclusion found in principle (e) of *PIPEDA* and therefore was not considered.

4.2.3 British Columbia

4.2.3.1 Common Law

The province of British Columbia adopted legislation to recognize the tort of invasion of privacy.[231] Although the *Privacy Act* does not define privacy, the recognition of the tort offers aggrieved plaintiffs a clear avenue of recourse.[232]

---

[230] See section 3.3, *below*.
[231] *Privacy Act*, RSBC 1996, c. 373.
[232] *Nesbitt v Neufeld,* 2010 BCSC 1605 at para 75, 194 ACWS (3d) 1333 (Here the Court states that the *Privacy Act* is the appropriate method to pursue an invasion of privacy).

The British Columbian case of *A T v L T H*[233] provides a good illustration of the diverse factors that must be considered when attempting to protect the privacy of an individual. The facts of *A T v L T H* are particularly interesting for this thesis as they involve the attempted publication of personal information on the Internet. The result in the case was the granting of an unusual injunction against the defendant mother preventing the publication of personal information regarding her daughter.

The Supreme Court of British Columbia (*BCSC*) confirmed the existence of the right to privacy in British Columbia as established through both common law and the *Canadian Charter of Rights and Freedoms*[234] (the *Charter*). The Court relied on sections 7 and 8 of the *Charter* to confirm that privacy was a value that requires protection.[235] While neither section 7 or 8 of the *Charter* explicitly states privacy as a right to be protected, the Court stated that such protection could be found in the right to liberty and the right to be secure. The Court being clear in its acceptance of protecting privacy stated "Respect for individual privacy is an essential component of what it means to be 'free'"[236]. This bold quote illustrates the importance in which privacy is regarded by the courts in Canada.

Importantly, it must be noted that the protection of privacy offered under the *Charter* and available under common law are not similar. The *Charter* may only be used in relation to

---

[233] *A T v L T H,* 2006 BCSC 1689.
[234] *Canadian Charter of Rights and Freedoms*, Part 1 of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), c 11.
[235] *Supra* note 233 at paras 20—23.
[236] *Supra* note 233 at para 23.

actions stemming from government that may restrict rights guaranteed under the *Charter*.[237] The common law right employed in *A T v L T H* can be used when the government is not a party to the action and therefore will be the relevant test when assessing right to be forgotten claims.

While recognizing the importance of protecting privacy, the Court is stating that no right is absolute and that it would need to be considered in light of:

a. the daughter having a reasonable expectation of privacy; and
b. other rights, such as freedom of expression, being balanced.[238]

In weighing this balance, the Court established that the daughter did have a reasonable expectation of privacy that outweighed her mother's right to freedom of expression.[239] In discussing the right to privacy, the Court noted that "once invaded, it can seldom be regained"[240]. This realization by the Court is important not only as an injunction was possible in *A T v L T H* but because it realizes a common consideration omitted from protection of privacy analysis at common law. The "irreparable harm"[241] created by the defendant mother publishing personal information online received weighty consideration in the case leading to the Court to state that "…the stigma and harm associated with this intrusion would be difficult, if not impossible, to remedy at a later time"[242].

---

[237] *Supra* note 234, s 1.
[238] *Supra* note 233 at para 25.
[239] *Ibid* at para 54.
[240] *Ibid* at para 23.
[241] *Ibid* at para 48.
[242] *Ibid* at para 48.

As stated above, the Court granted an injunction preventing the publication of personal information about the daughter. The Court carved out an exception to the injunction to allow the defendant mother to communicate (including by email) with immediate family and other mutually agreed persons regarding the daughter.[243] While this is a pragmatic solution by the Court, caution must be urged when carving out exemptions to injunctions relating to online publications. In *A T v L T H* the Court got it right, but such pragmatic solutions must be carefully crafted. The ease of sharing on the Internet could make an injunction futile if a person who was subject to the carved out provisions in the injunction accidentally (or purposefully) disclosed information being sought to be protected. Courts must fully understand the characteristics of the Internet when analyzing privacy and possible intrusions. Once the cat is out of the bag it is near impossible to put it back in.

The recent case, *Equustek Solutions Inc v Jack* (*Equustek),*[244] from the Court of Appeal of British Columbia (*BCCA*) also highlights the difficulties of applying injunctions on the Internet. The Court of Appeal granted a global injunction against Google preventing it from displaying search results related to the defendants on all of its top-level domains. The case has recently been appealed to the Supreme Court of Canada, where the Court will examine the application of Internet injunctions globally. *Equustek* is discussed in depth at section 5.1.2.3 of this thesis.

---

[243] *Ibid* at para 80.
[244] *Equustek Solutions Inc v Jack,* 2015 BCCA 265, [2015] 11 WWR 45.

4.2.3.1.1 Common Law and the Right to be Forgotten

The Court's recognition of privacy protection in British Columbia follows the approach seen in New Zealand and Ontario. The recognition of privacy is not absolute in British Columbia and must be assessed in accordance with a reasonable expectation of privacy. As already discussed, such an assessment is absent from the right to be forgotten, differentiating the approach in British Columbia from the *Regulation*. Without an expectation of privacy, courts in British Columbia will not invoke privacy protection. This additional requirement by the courts highlights, again, the departure the right to be forgotten is attempting to thrust upon the Internet and jurisdictions across the world. Under the current rationale, it is difficult to comprehend the current drafting of the right to be forgotten to be adopted in British Columbia, in particular if the personal information at issue does not attract a reasonable expectation of privacy.

Despite the absence of a reasonable expectation of privacy, the injunction awarded by the Court of Appeal in *Equustek* displays that global injunctions can be granted in British Columbia. As already stated, Article 17 can only be truly effective with global implementation. As privacy was not applicable to *Equustek* it must be distinguished from cases involving intrusions upon privacy. However, it does highlight that the Court of Appeal is willing to grant a global injunction against Google. Such an injunction runs parallel to the remedy available under Article 17 and signals that courts in Canada may be willing to adopt an Article 17-like remedy for privacy intrusions. While the remedy available in British Columbia is seemingly aligned with the *Regulation*, a reasonable expectation of privacy must still be established before any remedy may be awarded.

4.2.3.2 *Personal Information Protection Act*

Similar to Quebec, British Columbia has adopted its own version of the *PIPEDA* with the introduction of the *Personal Information Protection Act*[245] (the *PIPA*). The *PIPA* follows the same principles as seen in Quebec and in the federal *PIPEDA* with its primary focus being the protection of personal information balanced with an organization's ability to collect, use and disclose that information.

The *PIPA* relies on the following general concepts to ensure those competing values are achieved:

a) An organization must have consent of the individual to collect, use or disclose personal information;[246]
b) An organization must only use personal information for the purposes it disclosed to the individual;[247]
c) An organization must only disclose personal information for the purposes consented to by the individual;[248] and
d) An individual has the right to access and request a correction of the personal information held by the organization.[249]

---

[245] *Personal Information Protection Act*, SBC 2003, c 63.
[246] *Ibid*, s 10.
[247] *Ibid*, s 14.
[248] *Ibid*, ss 17-22.
[249] *Ibid*, s 24.

Helpfully, the *PIPA* provides a definition of organization broadly but excludes a person acting in a personal or domestic capacity.[250] Much like the federal and Quebec legislation, the *PIPA* is intended for the protection of personal information from unauthorized use within the private sector.

4.2.3.2.1 *PIPA* and the Right to be Forgotten

The *PIPA* only goes partially toward the protection currently offered by the right to be forgotten. Unlike the right to be forgotten, there is no provision in the *PIPA* for personal information to be removed. Rather, section 24 provides an individual with the right to request a correction of personal information.[251] While this provides some comfort to individuals to ensure their personal information is not misleading, it is still a big leap between correcting personal information and having it removed. Similar to the discussion above in relation to the *PIPEDA* in Ontario, the *PIPA* creates interesting tension in a right to be forgotten world. Section 14 provides that personal information can only be used for the purposes that were disclosed to the individual. However, in relation to a search engine, typically there will be no relationship between the individual, the third party who hosts the content, and the search engine operator. Without such a relationship, it becomes difficult for the search engine operator first to know what the purpose of the personal information was, and second to disclose that personal information within that purpose. In comparison, the right to be forgotten does not stipulate any communication between the multiple parties involved in a search request.[252] Somewhat

---

[250] *Ibid*, s 1.
[251] *Ibid*, s 24.
[252] *Supra* note 21 at 3.

differently, the EU, in its limited guidance on the right to be forgotten, urges that no communication take place between the search engine operator, the third party and the user. The *PIPA* is an example of the gap between technology and the law. We see here, that legislation has not fully comprehended the complex environment of the Internet. While the right to be forgotten is an attempt at tempering this unruly environment, it too has its own foibles, which are discussed in Chapter 5.

4.2.4 Table 4-1 Privacy Remedies Available Across Chosen Jurisdictions

Table 4-1 summarises the various protections available for an intrusion upon privacy across the jurisdictions of New Zealand, Quebec, Ontario and British Columbia. Noticeably, the *Regulation* is the only available remedy where personal information can be removed from the Internet. The *Regulation* goes beyond the current remedies available throughout the chosen jurisdictions, highlighting that the Internet has created unique problems for protecting privacy.

In comparison with the remedies available through the courts in all 4 jurisdictions, where injunctions may be granted, Article 17 not only side steps the judiciary but also amplifies on the remedy of an injunction as it attempts to regulate search engine operators globally.

Table 4-1 Privacy remedies available across chosen jurisdictions

Privacy Protection Available	**Remedy for Invasion of Privacy available through courts**	**Correct personal information held without court intervention**	**Limit access and disclosure of personal information held without court intervention**	**Removal of personal information without court intervention**
New Zealand	◉ Tort of Invasion of Privacy recognized	◉ *NZ Privacy Act*	◉ *NZ Privacy Act*	
Quebec	◉ Invasion of Privacy recognized in Quebec Charter	◉ Quebec Private Sector Privacy Act	◉ *Quebec Private Sector Privacy Act*	
Ontario	◉ Tort of Invasion of Privacy recognized	◉ *PIPEDA*	◉ *PIPEDA*	
British Columbia	◉ Tort of Invasion of Privacy recognized	◉ *PIPA*	◉ *PIPA*	
European Union's Right to Be Forgotten				◉ Article 17, the *Regulation*

4.3 Wholesale Adoption of a Tort of Invasion of Privacy

The three provinces examined all recognize that privacy is something, when intruded upon, that needs protection. While British Columbia[253] and Quebec[254] have legislated the protection of privacy in their respective domestic legislation, Ontario has adopted a tort of invasion of privacy (or seclusion) at common law. The adoption of a tort, as the Court of Appeal in Ontario recently recognized, provides greater ability for the court to mold the protection of privacy. This was exactly the result that occurred in *Jones v Tsige*. While British Columbia and Quebec provide protection for intrusion into one's privacy, adopting an intrusion tort at common law (in British Columbia) would assist with the fine-tuning of the protection around considerations such as the degree of damage required to a plaintiff and the balancing act that must be undertaken when competing values are being considered. For the purposes of this thesis, a unified approach to how the courts assess one's expectation of privacy (as discussed in British Columbia and Quebec) and whether it was 'highly offensive' (as adopted in *Jones v Tsgie*) would enable greater clarity when examining those factors in light of the intrusions of privacy on the Internet.

4.4 Understanding a Reasonable Expectation of Privacy

Both Canada and New Zealand include a reasonable expectation of privacy (highly offensive intrusion in Ontario) assessment to take place when evaluating one's right to privacy, whereas the right to be forgotten does not. Despite its absence from the *Regulation,* it is important to expand on what should be considered when making an assessment of a reasonable expectation of

---

[253] *Supra* note 185.
[254] *Supra* note 186.

privacy. The reasonable expectation of privacy test was first developed in the US case of *Katz v United States (Katz*[255]*).* In *Katz,* the Court developed a two-pronged test that is still widely used inside the US as well as in New Zealand[256] and Canada[257]. The two-pronged test asks whether:

a) A subjective expectation of privacy exists; and

b) Objectively, that expectation of privacy is reasonable.[258]

While none of the cases discussed above detail such considerations, the approach taken in *R v Tessling* (*Tessling*)[259] has framed the assessment developed by *Katz* with a six step assessment. The Court's assessment in *Tessling* can be summarised as an inquiry into, in the totality of the circumstances:

a) The place and subject and subject-matter of the search;

b) Whether the place and subject-matter were in the public view;

c) Whether the subject-matter had been abandoned;

d) Whether the subject-matter was subject to third party control;

e) The reasonableness of any technology used in the search; and

f) The nature of the information revealed.

---

[255] *Katz v United States*, 389 US 347 (1967).
[256] *Hosking v Runting,* [2004] NZCA 34 at para 117, [2005] 1 NZLR 1.
[257] *R v Tessling,* 2004 SCC 67 at para 19, [2004] 3 SCR 432.
[258] *Ibid* cf *Hosking v Runting,* [2004] NZCA 34 at para 117, [2005] 1 NZLR 1 (where the objective assessment focussed on publicity given to the private facts).
[259] *Supra* note 257.

Assessing a reasonable expectation of privacy is directly relevant to this thesis as including such an assessment within Article 17 of the *Regulation* would not only narrow the availability of Article 17 but also provide a greater understanding of how privacy is perceived on the Internet. Chapter 6 will explore the six step assessment in *Tessling* and examine how amending Article 17 of the *Regulation* would improve the current drafting of the right to be forgotten.

Chapter 5: Problems with the Right to be Forgotten

5.1 Critiquing the *Regulation*: Problems with the Right to be Forgotten

This Chapter of the thesis will discuss 3 key problems that the current drafting of the right to be forgotten presents not only within the EU, but also globally:

1 the danger of corporate censorship;

2 treating the symptoms and not the cause; and

3 the lack of unified jurisdiction.

It will outline how Article 17—in the hands of private business—will lead to a censored Internet as private businesses have little incentive to appropriately balance the competing rights relevant to a right to be forgotten request. Using examples of countries with heavy Internet censorship, this Chapter will illustrate how the *Regulation* could severely diminish an open and democratic Internet. This Chapter will discuss how Article 17 treats the symptoms only and does not prevent the cause of privacy intrusions on the Internet. It will discuss how the absence of a reasonable expectation of privacy furthers this problem and fails to contemplate how privacy is viewed by individuals on the Internet. Following this, it will discuss the futility of the *Regulation* where global enforcement cannot be achieved. The complex environment of establishing jurisdiction on the Internet may make the *Regulation's* application ineffective. In particular, the ease of circumvention that currently exists severely undermines the *Regulation.* This Chapter concludes with a discussion of a recent decision from the Court of Appeal of British Columbia outlining the complications of implementing a legal remedy across multiple jurisdictions.

5.2 Censorship

The concept of censorship is not novel, and has been a tool employed by society dating back to Plato.[260] Censorship, while applied differently across different jurisdictions, represents the removal or redaction of content that is deemed immoral, offensive or unacceptable. What is deemed unacceptable is vastly different across jurisdictions as each jurisdiction has its own unique culture and values that censorship attempts to protect. Although censorship is utilized for the protection of individuals, it is enforced through government. The government—representing the people—enforces censorship in relation to cinema, television, music, computer games and the Internet. As discussed in Chapter 2, the Internet represents a 'public' place where individuals instantaneously communicate across the world. In addition, the Internet is touted as being a bastion of free of expression and providing individuals with concrete (although virtual) access to information. However, the Internet can also be utilized as a tool for repression. The right to be forgotten challenges the values of freedom of expression and individual's right to access information as it will, when applied, censor the Internet. Worryingly for the Internet, this censorship will not be mandated by governments, but by rather private businesses such as Google. Not only is further censorship a cause for concern, especially in light of the Internet and its attributes, but shifting the burden of responsibility to private businesses aggravates this concern. The following section of this Chapter will discuss the current censorship taking place on the Internet and illustrate the how the right to be forgotten equates to additional and unwanted censorship.

---

[260] Yeen Fin Lim, *Cyberspace Law Commentaries and Material* (Oxford University Press: Melbourne, 2002) at 337.

5.2.1 Current Censorship on the Internet

China maintains the world's largest and most comprehensive censorship regimes, known as the 'Great Chinese Firewall'.[261] In addition, China reportedly has the largest number of imprisoned cyber-dissidents in the world.[262] The Chinese government dedicates considerable resources each year to filter and monitor the communication and content being transmitted through the Internet within China.[263] Particularly unnerving for Chinese citizens is the theme of censorship. Largely the Chinese government attempts to censor content and communication that relate to human rights. For example, there is no information available on the Internet in China about the horrific events that took place during the Tiananmen Square protests in 1989. Such is the depth of censorship in China that in 2013, when an artist supplanted Chinese military tanks with an inflatable big yellow duck onto the infamous images at Tiananmen Square of an unarmed student standing in front of the tanks, the Chinese government censored the search term 'big yellow duck'.[264]

The censoring of an innocuous phrase such as 'big yellow duck' from the Internet illustrates the dangers of censoring the Internet. Unlike traditional forms of media, the Internet is pliable lending itself to be easily censored without users being aware censorship has taken place. For

---

[261] Justine M Nolan, "The China Dilemma: Internet censorship and corporate responsibility" (2009) 4:1 Asian Journal of Comparative Law Article 3 at 3.
[262] Jessica E Bauml, "It's a Mad, Mad Internet: Globalization and the Challenges Presented by Internet Censorship" (2011) 63:3 Fed Comm LJ 697 at 704.
[263] *Supra* note 261 at 4.
[264] Michael B Kelly, "China Blocks Searches for 'Big Yellow Duck' After Brilliant Tiananmen Square Pun" *Business Insider* (4 June 2013), online: <http://www.businessinsider.com/chinese-censors-block-big-yellow-duck-2013-6>.

example, when users entered 'big yellow duck' into Chinese search engines, they received an error message akin to what an Internet user would view when attempting to view a deleted website. Therefore, users are not informed that the information has been subject to censorship, but rather may simply think they have entered a search term that has no results or a website that no longer exists. Unlike censorship of traditional media, which is palpable and therefore can be subject to public resistance,[265] censorship on the Internet is significantly less public and therefore can go unnoticed. The EU's *Working Party*, which provided guidance on the right to be forgotten in relation to *Google Spain*, furthers this practice and states that communicating to users of the Internet that personal information has been de-listed would undermine the right to be forgotten.[266] This recommendation by the *Working Party* intensifies and attempts to cement the dubious process of not providing notice to users of the Internet when de-listing personal information from the Internet. Not providing notice when censoring the Internet is particularly troubling as the architecture of the Internet means that users are unaware that information has been removed unless it directly affects them. As the right to be forgotten has the potential to affect freedom of expression and an individual's right to the access of information, there is a need for any limitation on such rights to be communicated. Such communication is ordinary in a judicial process, but the right to be forgotten takes place completely outside the domain of the judiciary instead being facilitated entirely by private businesses.

---

[265] Eric Fish, "Internet Censorship and Democracy in South Korea" (2009) 2 Asia-Pacific Journal on Human Rights and the Law 43 at 48 (For example, the 1979 Formosa incident in Taiwan where censorship relating to a magazine sparked protest that has been attributed to the eventual establishment of democracy within Taiwan).
[266] *Supra* note 21 at 9.

In addition to the Chinese government's well resourced censorship regime, the regulations that mandate such censorship are deliberately vague.[267] The Chinese government, among other things, seeks to censor any information that "might harm the state's honor, cause ethnic oppression, spread rumours, disrupt social stability, spread pornography, undermine state religious policy, or preach the beliefs of evil cults"[268]. The presence of vague regulations provides China with more room to censor on the Internet, somewhat contrasted with what westernised democratic citizens expect when human rights are being impaired. In Canada and New Zealand, any restriction on rights such as freedom of expression must be proportional to the harm felt.[269] However, in China there seems to be no attempt to ensure that rights such as freedom of expression are restricted proportionally to the objective of the restriction. The opposite appears to be true in relation to China. Not only do the vague regulations provide the Chinese government with more scope to censor the Internet, but also effectively force foreign Internet intermediaries to over-comply with censorship regulations to maintain their licence in China.[270] Without clear regulations as to what must be censored, Internet intermediaries—under the fear of liability and loss of their ability to do business in China—will censor content and communications that are outside of the black letter of the Chinese censorship programme. The presence of vague wording is also found in the *Regulation*, namely found in article 17 where personal data may be erased if it is "no longer necessary". It would be a downward spiral for the

---

[267] *Supra* note 262 at 705.
[268] Human Rights Watch, "Race to the Bottom; Corporate Complicity in Chinese Internet Censorship" (2006) Human Rights Watch Report 18:8 at 18.
[269] *Supra* note 155 at para 41; *Supra* note 209 at para 734.
[270] Max Rothschild, "Corporate Cyber-Censorship: The Problems with Freedom of Expression Online" (2013) 11 CJLT 143 at 151.

Regulation and the EU to fall into if they began heading in the direction China takes with its vague Internet regulation.

Internet intermediaries in the Chinese market are complicit in the oppressive censorship because of the value of the Chinese economy.[271] The censorship employed by China is drastic, offends multiple human rights but has the potential to make Internet intermediaries substantial revenue. While there are still a large number of 'big players' (Twitter, Yahoo and Microsoft) operating within China, Google exited China in 2010 in favour of basing its Chinese operations in Hong Kong.[272] Unlike China, there are no censorship restrictions in Hong Kong. Users may search information and images relating to Tiananmen Square or big yellow ducks without such content being blocked by the Great Chinese Firewall. While Google exited China in 2010, the presence of the remaining Internet intermediaries illustrates the continued compliance with the Chinese government and continued oppression of the Internet users in China. While the Great Chinese Firewall is mandated by the Chinese government, much of its enforcement is through Internet intermediaries.[273] The current practice in China is set to expand under the right to be forgotten. Similar to the practice currently in China, the right to be forgotten prescribes that data controllers (private business) must erase content from a right to be forgotten request rather than being implemented through government. Although the extent of who is and is not a data controller is yet to be established, we do know that search engines such as Google fall into the category.[274]

---

[271] *Supra* note 261 at 4.
[272] *Supra* note 262 at 727.
[273] *Supra* note 261 at 5.
[274] *Supra* note 11 at paras 21—44.

The right to be forgotten passes the burden of censorship onto private organisations and therefore shirks governments' responsibility to uphold fundamental human rights.[275] The right to be forgotten will parallel censorship on the Internet, when applied, as it de-lists certain information from search engine websites.

5.2.2 The Right to be Forgotten and Censorship

The right to be forgotten seeks to de-list certain personal information from the Internet. The operative word being "de-list". Although this word is not found within Article 17—but rather "erasure"[276]— it describes an act where personal information will be removed from search engine results but remain on the Internet. This interesting dynamic between being on the Internet but not searchable or accessible begs the question as to whether such information is still—practically speaking—on the Internet or whether de-listing amounts to censorship. A purpose for the introduction of the right to be forgotten, among others, is to return individuals to 'practical obscurity'.[277] Practical obscurity amounts to when although personal information is publicly available (i.e. through the Internet), it is not accessible or searchable because of the vast amounts of other information readily available that obscure the personal information. In the case of information that becomes subject to the right to be forgotten, de-listing not only makes it practically obscure, but goes further and makes it unavailable.

---

[275] Dawn C Nunziato, "How (Not) to Censor: Procedural First Amendment Values and Internet Censorship Worldwide" (2011) 42:4 Geo J Int'l L 1123 at 1130-1135 (168 countries are a party to the International Covenant on Civil and Political Rights and a further 47 countries have signed the European Convention for the Protection of Human Rights, both which protect freedom of expression).
[276] *Supra* note 4 at 43, see art 17.
[277] *Supra* note 96.

While critiques of this argument may state that the right to be forgotten does not amount to censorship as the information remains on the Internet, this position is unrealistic. Search engines since their inception have become the ubiquitous tool for navigating the Internet. Google consistently tops the world's most visited websites,[278] in addition 8 out of the top 20 websites visited globally are search engine websites.[279] The remainder of the 20 top sites visited globally are largely made up of SNWs such as Facebook, Twitter and LinkedIn.[280] It is unclear whether such websites will also be deemed data controllers and therefore subject to the right to be forgotten. Regardless of the inclusion of popular SNWs in the top websites visited globally, search engine websites provide the portal to the Internet. Without search engine websites, the Internet would become a random, unorganized and unhelpful technology. As stated by Justice Binnie in *Society of Composers, Authors and Music Publishers of Canada v Canadian Assn. Of Internet Providers* (*SOCAN*)[281] the "capacity of the Internet to disseminate "works of the arts and intellect" is one of the great innovations of the information age".[282] Although *SOCAN* related to intellectual property rights, the comments by Binnie J remain pertinent for this Chapter. Dissemination through the Internet is largely achieved because of the ease by which information can be searched, located and accessed. Restricting information and de-listing information from search engines goes against this concept of dissemination, making it harder to search, find and access information and therefore hampering the great technological advances currently celebrated by users of the Internet.

---

[278] Alexa, "The Top 500 Websites on the Web", *Alexa* (website) online: < http://www.alexa.com/topsites> (Google was visited by over 180 million unique visitors in December 2015).
[279] *Ibid*.
[280] *Ibid*.
[281] *SOCAN v Canadian Association of Internet Providers*, 2004 SCC 45, 32 CPR (4th) 1.
[282] *Ibid* at para 40.

The process for de-listing information, as discussed in Chapter 3, further illustrates how the right to be forgotten will haphazardly censor the Internet. Similar to the process adopted under the *Digital Millennium Copyright Act* (the *DMCA*)[283], which was enacted in 2000, the process under the right to be forgotten creates incentives for the rapid removal of 'infringing' content.[284] Section 512 of the *DMCA* creates a safe-harbour for Internet service providers who "expeditiously" remove content that infringes copyright. Similar wording is found in Article 17 of the *Regulation*, where data controllers must "…erase personal data without undue delay…"[285]. Before discussing the analogies between the *DMCA* and the *Regulation*, we should pause to consider the focus on time under both regimes. The *DMCA* and section 512 relate to copyright law, a topic that is not known for its clarity. Defences to copyright infringement include 'fair use', an extremely nuanced legal assessment that does not sit comfortably in a 'time is of the essence' evaluation. Such are complexities of fair use that YouTube has publicly commented that it cannot always assess whether a video qualifies as fair use.[286] In its admission, YouTube stated that rather than further examine the fair use of each video, it removed all videos that the take-down notice related to.[287] Similarly, the *Regulation* and the right to be forgotten must consider the equally complex concepts of freedom of expression and information. Again, another area of the law that is fraught with subtleties and is highly contextual. Having to remove

---

[283] *The Digital Millennium Copyright Act,* 17 USC § 512 1998.
[284] *Ibid*; *Supra* note 4 at 43, see art 17 (Data controllers must remove infringing content with "undue delay").
[285] *Supra* note 4 at 43, see art 17.
[286] Julie Alder, "The Public's Burden in a Digital Age: Pressures on Intermediaries and the Privatization of Internet Censorship" (2008) 20 JL & Pol'y 231 at 247.
[287] *Ibid*.

content from the Internet "without undue delay" illustrates the mismatch between the clear rigid process of the right to be forgotten and the nuances of human rights law.

Not only is speed an incentive that is spelled out under Article 17,[288] it is coupled with the scale of fines prescribed by the *Regulation*, it is hard not to imagine the severe chilling effect taking place as personal information is de-listed from the Internet out of apprehension of the fines. Article 79(3a)(b) states that an infringement of Article 17 will lead to a fine of up to 20 million euros or 4% of worldwide turnover, whichever is greater.[289] In relation to Google, 4% of worldwide turnover would amount to 1.5 billion US dollars for the year 2015.[290] Faced with such massive liability, it is not difficult to imagine a landscape where personal information is removed from search engines in a similar approach to that undertaken by YouTube under the *DMCA*. The complexity of assessing whether removing personal information will infringe freedom of expression and the fear of massive pecuniary fines leave search engines with little room but to remove content that may not be applicable to the right to be forgotten. The *Regulation* is tilted toward quick removal for the protection of the individual and their personal privacy, but does not consider the scope of the effects when data controllers are incentivised to quickly remove personal information. Similar to the *DMCA*, there is no reverse onus provision in the *Regulation*. Under the *DMCA*, the safe-harbour can only be obtained if the Internet intermediary removes the content "expeditiously"[291]. If they do not comply with the timely

---

[288] *Supra* note 4 at 43, see Article 17.
[289] *Ibid* at 82, see art 83.
[290] Alphabet Investor Relations, Press Release, "Alphabet Announces Fourth Quarter and Fiscal Year 2015 Results" (1 February 2016), online: Alphabet Investor Relations <https://abc.xyz/investor/news/earnings/2015/Q4_google_earnings/index.html>.
[291] *Supra* note 283.

process, liability may be attributed to the Internet intermediary. Internet intermediaries must therefore err on the side of caution to avoid the risk of liability. The *Regulation* does not contain any 'stand down' period where content may be assessed by the search engine leaving search engines in the same position as Internet intermediaries under the *DMCA*. A recent study into a selection of *DMCA* takedown notices revealed that one third had a substantial legal flaw, either in relation to the legality of the takedown notice or technical noncompliance with the *DMCA* procedure.[292] Despite these flaws, the content concerned by these *DMCA* takedown notices has been removed from the Internet. This 'shoot-first ask questions later' approach is both unwise and dangerous for the Internet. While the *Regulation* states that the right to be forgotten does not apply to personal information that is exercising freedom of expression and information, the reality of a private business getting that assessment right is proven in the *DMCA* context to be more difficult than prescribed by the *Regulation*.

5.3 Treating the Symptoms not the Cause

Article 17 of the *Regulation* fails to contemplate how an individual on the Internet understands privacy. Currently, the wide drafting contained in the *Regulation* allows for Article 17 to apply to any personal information.[293] This is contrasted with the jurisdictions examined in this thesis,[294] where a reasonable expectation of privacy must be established before any remedies are granted. The absence of a reasonable expectation of privacy treats all personal information the

---

[292] Jennifer M Urban & Laura Quilter, "Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act" (2006) 22 Santa Clara Comp & High Tech LJ 621 at 666.
[293] *Supra* note 4 at 33, see art 4.
[294] See Chapter 4, *above*, for more on this topic.

same despite individuals not expecting that all their personal information on the Internet should attract privacy protection. The growth of SNWs and individuals publishing content on SNWs has seen a shift in how individuals value privacy on the Internet. While the high level of content being published has led the EU to hold that all personal information should attract privacy protection, such an assumption devalues privacy on the Internet. The genesis of this assumption can be found in the belief that the over-sharing culture of the Internet has equated to a complete loss of privacy. This was highlighted in the now-famous quote by Scott McNealy (then CEO of Sun Microsystems) to claim "you already have zero privacy – get over it"[295]. Such belief has seen the EU to claim—in its definition found in the *Regulation*—that all personal information can receive privacy protection. However, while individuals are sharing personal information on the Internet this does not equate to that personal information being private.[296]

The *Regulation* does not—in the absence of a reasonable expectation of privacy assessment—look to the intention of the individual when the personal information was shared. This failure to assess whether there was an expectation of privacy in relation to the personal information and rather assume that it does confuses the concept of privacy. As discussed in Chapters 2 and 3 of this thesis, privacy is a concept that is largely contextual and does take on different meanings. However, just because it can take on different meanings because of the context does not warrant a blanket assumption that all personal information is private. Rather, it should mean the opposite. That while personal information may have an expectation of privacy for one

---

[295] Lisa M Austin, "Privacy and the question of Technology" (2003) 22:2 McGill LJ 167.
[296] *Supra* note 69 at 241.

individuals or section of society, the same personal information may not for different individuals and sections of society. In adopting the approach by the EU, privacy risks becoming meaningless on the Internet, as making privacy protection available for all and sundry does not align with both how individuals on the Internet view their privacy and modern definitions of privacy. This devalues privacy as Article 17, pragmatically, becomes more about the ability to remove unwanted content than valuing privacy. Modern understandings of privacy are extremely contextual and this is more pertinent on the Internet. Rather than look to whether the relevant information is personal and therefore subject to Article 17, the assessment should be whether there was a desire for something to be kept private.[297] This assessment actually aligns with how individuals use the Internet as much information published will fit within the definition of personal information found in the *Regulation* but will not fit with the individual's intention behind that publication.

This wide definition of personal information absent any other qualifications typically found in a privacy intrusion fact pattern highlights the little concern the *Regulation* actually has for the protection of privacy. It masquerades as a bastion of privacy protection but has not considered what privacy means on the Internet. What and how privacy is and can be represented on the Internet must be the focus as without coherence and understanding, privacy intrusions will continue to intensify. The end goal—of providing greater control to individuals—cannot be undermined but that control should not applicable to all content relating to individuals on the

[297] Brandon T Crowther, "(Un)reasonable Expectation of Digital Privacy" (2012) 1 BYU L Rev 343 at 346.

Internet. Such an application overlooks the value of privacy and the discussion that is needed as to what is private on the Internet in favour of a quick fix. Chapter 6 will further discuss how a reasonable expectation of privacy can strengthen social and individual's understanding of privacy on the Internet and align privacy protection with Internet culture.

5.4 Jurisdiction of the Right to be Forgotten

As mentioned above in Chapter 3, while the *CJEU* did not provide any extensive criteria of how the right to be forgotten should be implemented, the *Working Party* did.[298] One area for strong contention is the territorial reach that the right to be forgotten, as interpreted by the *Working Party*, attempts to capture. The *Working Party*, under the important guise of effectiveness, states that removing requested content from all top-level domain names, not just those within the EU, is the only way to achieve the goal of the right to be forgotten.[299] The *Working Party* is not wrong, but such a task underscores one of problems of the right to be forgotten. Countries outside the EU that are connected to the Internet may not be willing to cede sovereignty in favour of enforcing EU legislation domestically.[300] In doing so, the Internet challenges the applicability of decisions such as *Google Spain* and typically finds a way around the domestic ruling.

---

[298] *Supra* note 21.
[299] *Ibid* at 3.
[300] M L Rustard, *Internet Law in Nutshell,* 2nd ed (United States of America: Thomson Reuters, 2009) at ch 3.

The *CJEU* in *Google Spain* established jurisdiction for Google and its subsidiary—Google Spain—as it was an establishment within the territory of a Member State (Spain).[301] While making this finding enabled the *CJEU* to apply the *1995 Regulation* to the factual analysis of the case, it did not extend enforcement beyond the EU. This extension was provided by the *Working Party* in its guidance on the *Google Spain* decision.[302] Establishing jurisdiction on the Internet is notoriously difficult as the Internet is not a physical space with sovereignty. Traditionally, jurisdiction relates to the sovereignty of a state and therefore exercising jurisdiction outside of that sovereignty should be approached with caution.[303] If a state wishes for their sovereignty and jurisdiction to be respected, it may assume that other states wish the same.

5.4.1 Establishing Jurisdiction over the Internet

Traditional methods for establishing jurisdiction must be altered when attempting to establish it over the Internet. As jurisdiction has been traditionally restricted to the geographical borders of a state, the borderless Internet requires new rules. Activity over the Internet does not occur in one place only, but occurs at the place where the information is transmitted and the place where it is received.[304] Rather than look to sovereignty as a indication of establishing jurisdiction, courts must assess a variety of different considerations when extending their jurisdictional reach beyond a state's borders.

---

[301] *Supra* note 11 at para 55.
[302] *Supra* note 21.
[303] Brendan Van Alsenoy and Marieke Koekkoek, "Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted'" (2015) 5:2 Intl Data Privacy L 105.
[304] F Lawrence Street & M P Grant, *Law of the Internet,* 2000 Edition (Virginia: Lexis Law Publishing, 2000) at 279.

Early Internet-jurisdiction cases looked at the interaction between the individual using the website and website provider as an indication of presence in a jurisdiction.[305] The concept of a continuing relationship was developed out of early cases that saw the focus on establishing jurisdiction as having sufficient minimum contact with the user and the state where that user was located.[306] However, this precedent was quickly developed and the focus shifted to how the parties had been affected.[307] The case of *Dow Jones & Company Inc v Gutnick* (*Dow Jones v Gutnick*)[308] cemented the 'effects test' as a measure for establishing jurisdiction on the Internet. The Court stated that as the appellant had felt the effects of the defamation in his home state of Australia, the claim should be tried in Australia only. The Court dismissed Dow Jones' argument that it should be regulated by the jurisdiction where its servers were located.[309] Instead, the Court stated that because the appellant knew its website could have worldwide reach, it would have to face foreign legislation when harm occurred to a user of their website.[310]

Similar to the decision in *Dow Jones v Gutnick,* the case of *Yahoo! Inc v La Ligue Contre Le Racisme Et L'Antisemitisme* (*Yahoo France*)[311] is an example of the problems created by the application of traditional legal rules to the Internet.[312] The facts concerned the online auction of Nazi memorabilia that were available on 'Yahoo.com' only and were not available on the French

---

[305] *Zippo Mfg Co v Zippo Dot Com Inc,* 925 F Supp 119 (WD PA 1997) (Here the Court established a 'sliding scale' for Internet jurisdiction between passive websites with little user interaction to interactive websites with interaction with users).
[306] *Supra* note 20 at 59-62.
[307] *Ibid* at 63.
[308] *Supra* note 72.
[309] *Ibid.*
[310] *Ibid.*
[311] *Yahoo! Inc v La Ligue Contre Le Racisme Et L'Antisemitisme,* 433 F3d 1199 (9th Cir 2006).
[312] *Ibid.*

subsidiary 'Yahoo.fr'. However, both websites 'Yahho.com' and 'Yahoo.fr' were accessible by individuals in France. The Court found that the sale of Nazi memorabilia through 'Yahoo.com' was illegal as it offended domestic legislation in France. Although the auction of Nazi memorabilia was not available through 'Yahoo.fr', it did not require much technical knowledge to access the sister 'Yahoo.com' website.[313] In making this decision, the French court applied the 'when in Rome' ideal to the Internet and believed that websites accessed by French residents should abide by French law. Yahoo rejected the French court's ruling on the grounds that it would offend the First Amendment of the *United States Constitution*.[314] While the French court's ruling was not ultimately enforced upon 'Yahoo.com', the auctions containing Nazi memorabilia were removed voluntarily by Yahoo. However, the genesis of the French court's ruling created problems for those who are connected to the Internet.

If developed into a precedent, any court may establish jurisdiction in relation to activities on the Internet and enforce jurisdiction over anyone else no matter their connection to the domestic jurisdiction.[315] Both *Yahoo France* and *Dow Jones v Gutnick* argued for establishing jurisdiction on the Internet as a result of the global reach of the websites on the Internet. Both cases highlight the complex position the Internet creates for the courts. There is a need to enforce domestic legislation as this is a role played by courts. This need, however, sits somewhat uncomfortably with the notion of the 'open Internet'. The openness and borderless environment of the Internet is a core value of the Internet and one that is often cited as being a key success of

---

[313] Adria Allen, "Internet Jurisdiction Today" (2001) 22:1 Nw J Intl L & Bus 69 at 71.
[314] *Supra* note 20 at 73.
[315] *Supra* note 313 at 75.

the Internet.[316] Restricting the openness of the Internet by making website providers and/or publishers subject to countless different jurisdiction will stifle that openness. Further, it may seem harsh to penalise someone under a foreign jurisdiction if they never intended to enter that jurisdiction.[317] While the end-goal in *Yahoo France* can surely be described as desirable, would the application of a conservative middle-eastern state's jurisdiction be as equally desirable?[318] It is here that the global application of domestic legislation reveals itself as a problem. Western nations (and member states of the EU) may be happy to accept the jurisdiction of each other under the international legal concept of comity,[319] but extending this wholesale to the Internet could be dangerous. Danger lies within the potential chilling effect that this approach to Internet jurisdiction could create. If content-hosts and publishers face costly legal risk with publication and facilitation of the Internet, it is inevitable that some players will drop out of the market.

5.4.2 Jurisdiction of *Google Spain*

The *CJEU* established jurisdiction for Google as it had a subsidiary within the EU that carried out activities substantially similar to those undertaken by itself.[320] The approach taken by the *CJEU* can be seen as being resonant of the effects principle developed in *Yahoo France* and *Dow Jones v Gutnick*. The harm was created within the EU to Mr. Gonzalez and therefore those who have created the harm (Google) should be subject to the law where the harm originated. While

---

[316] Raphael Cohen-Almagor, "Internet Architecture, freedom of expression and social responsibility: critical realism and proposals for a better future" (2015) 28:2 Innovation: The European J of Social Science Research 147 at 148.
[317] *Supra* note 304 at 280.
[318] *Supra* note 313 at 81.
[319] *Supra* note 20 at 73.
[320] *Supra* note 11 at para 55.

this finding, although important for the outcome of the case, did not extend the reach of courts powers outside of the EU jurisdiction, the *Working Party's* published guidance did. It is this extension that exacerbates the tension between enforcing domestic legislation and the openness of the Internet.

Similar to the arguments cited in *Yahoo France*, the application of *Google Spain* outside of the EU creates the same problems for constitutional rights such as freedom of expression. While any request to remove personal information from the results shown on search engine operators must be balanced against the competing rights such as freedom of expression,[321] this assessment is driven out of the EU and the relevant EU-law. To undertake this assessment outside of that jurisdiction may lead to vastly different results. In the United States, for example, the weight of the *Constitution* would most likely see the decision in *Google Spain* trumped by the right to free speech. The Supreme Court in the United States stated:

> …exposure of the self to others in varying degrees is a concomitant of life in a civilized community. The risk of this exposure is an essential incident of life in a society which places a primary value on freedom of speech and of [the] press.[322]

It is here that the clash between two different jurisdictions can be seen. A United States court, in all likelihood, would not arrive at the same result as the *CJEU* did in *Google Spain*. Yet the

---

[321] *Supra* note 11; *Supra* note 21.
[322] Robert G. Larson, "Forgetting the First Amendment: How Obscurity Based Privacy and a Right to Be Forgotten Are Incompatible with Free Speech" (2013) 18:1 Comm L & Pol'y 91 at 97.

United States and any other offending jurisdictions are expected to comply with the ruling. The *Working Party* made this clear – the removal of personal information must be completed for all top-level domain websites, not just those within the EU.[323] The rationale behind the *Working Party's* guidance to implement global application of the right to be forgotten may be seen as a solution to scenarios similar to that of Max Mosley.[324] Max Mosley, the former president of Fédération Internationale de l'Automobile (the non-profit organization that oversees international car racing such as Formula One), although being a EU resident is also well known outside of the EU. In such cases, the global implementation of personal information is the only way to effectively enforce protection on the Internet. As mentioned above, caution must be urged when attempting to extend jurisdictional reach outside a state's territory. While the EU is not known for regressive lawmaking, the potential danger of accepting other more conservative states' jurisdiction outside their own borders is worrying.

The *Working Party* guidance highlights a problem with the right to be forgotten and its effectiveness. This problem is not unique to the right to be forgotten but present in many attempts by courts to regulate the Internet. The ease by which the Internet can circumvent a legal rule is uncomplicated. As is the case for Mr. Gonzalez, the personal information he has had removed from the Internet only extended to top-level domain names within the EU. An individual within the EU can simply alter their target website's top-level domain from '.es' (Spain) to '.com' (United States) and access the 'deleted' information. Top-level domain name

---

[323] *Supra* note 21.
[324] *Supra* note 303 at 112.

identifiers, geography-blocking (geo-blocking) and wholesale deletion are the three most common ways of controlling jurisdiction on the Internet.[325] Google is employing two of three most common methods for controlling information flows within a jurisdiction under the *Google Spain* decision.[326] Top-level domain identifiers have been employed to ensure the removal of the personal information requested by Mr. Gonzalez from all of Google's EU top-level domain identifiers. In addition, Google is using geo-blocking to identify which of its users are within the physical borders of the EU and will subsequently automatically direct them to the correct top-level domain identifier. This means that without the individual user doing anything, they will automatically find themselves on the Internet where the personal information has been removed from Google's search results. However, as stated above, a user may alter their top-level domain name to a jurisdiction outside the EU and easily circumvent the right to be forgotten.

The third available method for controlling information within jurisdictions abandons the concept of jurisdiction as it requires that the information be completely removed from the Internet.[327] This method, which is stated by the *Working Party* to be the only effective method of achieving the goals of the right to be forgotten creates substantial problems on the Internet.

---

[325] *Supra* note 303.
[326] Google, "Are you removing pages wholesale from your search results?", *Google Transparency Report* (website), online: <https://www.google.com/transparencyreport/removals/europeprivacy/faq/?hl=en#are_you_removing>.
[327] *Supra* note 303.

5.5 Whack-A-Mole: Toward Global Implementation

The Canadian case of *Equustek Solutions Inc v Jack (Equustek)*[328] saw a global injunction ordered against Google as the *BCSC* referenced the borderless environment of the Internet.[329] The *BCSC* went on to state that the geo-blocking by Google was insufficient protection for the plaintiff as such protection was easily circumvented. The *BCSC* built on this argument in stating that a global injunction was needed as laws of other sovereign states had also been breached.[330] On appeal, the Court reiterated that geo-blocking was insufficient as the removal of any content from Canadian websites was met by the defendant simply uploading the infringing content to new websites that were not subject to the restriction.[331] Such behaviour led the frustrated appellants to state that they felt as if they were playing a game of Whack-A-Mole[332] with the Internet. The *BCCA* affirmed the decision of the *BCSC* in finding that Google could be subject to its jurisdiction as it has a real and substantial connection to British Columbia.[333] Similar to the finding in *Google Spain*, the *BCCA* held that the technology employed by Google within Canada to operate its search engines and its Canadian-specific advertising gave the Court jurisdiction over Google within British Columbia.[334]

Unlike the *Working Party* which is concerned for the effectiveness of the right to be forgotten only, the *BCSC* in *Equustek* took into account a variety of relevant factors including:

---

[328] *Supra* note 244.
[329] *Ibid* at para 159.
[330] *Ibid.*
[331] *Ibid* at para 25.
[332] Whack-A-Mole is an arcade game in which players use a mallet to hit toy moles, which appear at random, back into their holes.
[333] *Ibid* at para 29.
[334] *Ibid* at para 55.

(a) whether the interests of justice favour the granting of the relief sought; and

(b) the degree to which the interests of those other than the applicant and the identified non-party could be affected.[335]

The factors developed by the *BCSC* identify important considerations that must be assessed before a court impinges on the national sovereignty of another state. In comparison to top-level domain identifiers and geo-blocking, global implementation of jurisdiction on the Internet may infringe on another state's sovereignty and territory. This fact was noted by the *BCCA*, in stating that the worldwide implementation of injunctions can cause problems,[336] a comment noticeably missing from the *Google Spain* decision and the *Working Party* rhetoric. The *BCCA* explicitly mentions that because of the importance that different states place on freedoms such as freedom of expression, caution must be urged when granting injunctions with worldwide reach.[337]The Court went on to note that the facts of *Equustek* did not evoke such problems and the injunction would not infringe on other states' values or freedoms.[338]

Equustek has recently been appealed by Google to the Supreme Court of Canada where the decision of the *BCCA* will be revisited. The result of the appeal will alter the development of Internet jurisdiction cases and if dismissed, affirm acceptance of the current global approach taken by the *BCSC* and *BCCA*. The appeal is expected to be heard in the second half of 2016.

---

[335] *Ibid* 154—155.
[336] *Ibid* at para 56.
[337] *Ibid* at paras 91—92.
[338] *Ibid* para 93.

Anxiety remains as to whether the decision will be affirmed, as doing so could open the doors for a court to delist entire domains from search results for reasons that lay closer to constitutional protections such as free speech.

Another British Columbia case, *Niemela v Malamas (Niemela*)[339] also involves an injunction sought by the plaintiff against Google to block information from its global search results. Unlike *Equustek*, the *BCSC* did not permit the injunction and continued to allow Google to block only search results within Canada.[340] Interestingly for this thesis and the *Regulation*, the Court stated it did not want to grant an injunction that cannot be complied with. Such sentiment is an important consideration when making a ruling involving the Internet. As stated above, the Internet does not operate within a physical space, which frustrates traditional legal doctrines such as jurisdiction. The Court stated in *Niemela* that granting a worldwide injunction would be fruitless as countries such as the United States would not enforce foreign rulings that infringe freedom of expression.[341] Further, the Court noted that Internet search engine operators command an important role on the Internet, and injunctions such as the one sought in *Niemela* could be threating for the Internet as compliance and liability increase.[342]

The differing results in *Equustek* and *Niemela* highlight the complex environment the courts find themselves in with the Internet. With establishing jurisdiction, there is a fine balance to be met

---

[339] *Niemela v Malamas,* 2015 BCSC 1024.
[340] *Ibid* at para 31.
[341] *Ibid* at paras 33—34.
[342] *Ibid* at paras 101—102.

between enforcement and effectiveness. The decision in *Equustek* provides for the possibility that the *Regulation's* jurisdictional reach would be accepted in Canada. However, *Equustek* will most likely be limited to its facts as the elements such as the continued uploading of infringing information and the little value in the expression guided the *BCCA* to their decision. In contrast, *Niemela* provides little hope for the jurisdictional reach recommended by the *Working Party*. The Court in *Niemela* focussed on the effectiveness of an injunction that would simply be ignored by foreign courts. This pragmatic understanding is the same understanding overlooked by the *Working Party* in their attempt to extend the reach of *Google Spain* and the same understanding that prevented global implementation in *Yahoo France*.

Global implementation requires removal of the relevant personal information on all available websites provided by a search engine operator. Such implementation is difficult to establish as there are vast considerations that must be taken into account, effectiveness being central to those considerations. Global implementation is either off or on. The right to be forgotten cannot be effective without global acceptance, if one country—for example the Unites States protecting freedom of expression—does not comply, the remedy is ineffective. Additionally, global implementation can be dangerous for the Internet as society experiences it today, increasing global reach of domestic law muddies the water further and runs the risk of a potential 'chill' on how the Internet functions.

Chapter 6: Where to Now?

This Chapter argues that the problems highlighted in Chapter 5 can be mitigated by amending the *Regulation* and in particular Article 17. Chapter 5 outlined that the *Regulation,* as currently drafted, is a partial solution only. Chapter 6 discusses how the *Regulation* can become an effective solution for intrusions of privacy on the Internet. It will argue for a co-regulatory approach where search engine operators and government collaborate to ensure that not only the *Regulation* is enforced but also promotes transparency and due process. This Chapter will also introduce the need for a remedial process within the *Regulation* and argue that such a process is imperative when fundamental values are being assessed completely absent of the judiciary. It will conclude with a call to amend Article 17 to include a reasonable expectation of privacy assessment. Such an assessment will reduce the scope of Article 17 and better align social expectations of privacy with the *Regulation.* This Chapter will argue that the amended Article 17 must include a modified reasonable expectation of privacy assessment that is unique to the Internet.

6.1 Building a Better Model

The preceding Chapter highlighted critiques of the right to be forgotten, this Chapter will focus on how to temper those problems. Primarily this Chapter will argue for amendments to the *Regulation*. This Chapter will also focus on the vague drafting of the *Regulation* and will argue that the following amendments should be made:

a) Introduce a corporate social responsibility (*CSR*) regime to the *Regulation* that ensures basic legal rights are respected; and

b) Introduce a reasonable expectation of privacy into Article 17.

6.2 Google the Gatekeeper

As has been discussed in Chapter 5 the *Regulation* does not provide an adequate solution for the current harm occurring through the Internet. Although there are other limitations of the *Regulation*, the risk of censorship, devaluing privacy and the lack of enforcement all lead to a need for the *Regulation* to be amended. An amendment to the *Regulation* is needed to ensure that the Internet-only right has crucial buy-in from the major players of the Internet and, in particular, search engine operators. Google is consistently the world's most visited website with over 1.17 billion unique visits per month.[343] Google is not the only search engine in operation, but as it is the largest, it will be the focus of this Chapter.

With so many unique visits each month, Google is responsible for the navigation of 1.17 billion individuals through the Internet. Google determines where they go on the Internet and what they access on the Internet. The sheer volume of users to Google's websites indicates the democratic participation taking place through the Internet.[344] Because of this role Google has as—in 1.17 billion instances—a first point of contact on the Internet, its role is analogous to that of a gatekeeper.

---

[343] Craig Smith, "By the Numbers: 100 Shocking Google Statistics and Facts" (14 July 2016), *Expanded Ramblings* (blog), online: < http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts/>.
[344] *Supra* note 3.

Gatekeepers, at a broad level, are the organizations that determine who may pass through a gate. Uniquely gatekeepers typically will have no continued relationship with those who pass through their gate, once they have either passed through or been denied entry.[345] While being immune from the behaviour of those who pass through the gate, gatekeepers are in a powerful position to regulate behaviour by incorporating controls at the gate.[346] An example of effective controls that curtailed bad behaviour can be seen in the oil tanker industry.[347] With the goal of reducing oil spills through top-down legal regulation on oil tankers and their owners being ineffective, the industry decided to instead regulate the gatekeeper: the insurers.[348] In this example, the insurers were only able to insure oil tankers that had separate ballast tanks, which in turn led to a change in building practices worldwide so as to obtain insurance, safer oil tankers were built leading to a 98% compliance.[349] As mentioned above, Google can be portrayed as a gatekeeper as it a non-state actor that has the ability to alter the behaviour of users who visit its search engine website. And importantly, it determines which information may pass through its search engine.

As a result of this role, Google also facilitates or impedes highly valued human rights such as privacy and freedom of expression. If Google decides to remove content from its search engine as a result of the *Regulation* or continues to allow access to content that should be removed, it is making a judgement call on whether such content attracts protection from freedom of expression or privacy. Such a decision, on whether a human right is being facilitated or impeded has been

---

[345] Emily B Laidlaw, *Regulating Speech in Cyberspace Gatekeepers, Human Rights and Corporate Responsibility* (United Kingdom: Cambridge University Press, 2015) at 37.
[346] *Ibid*.
[347] *Ibid*.
[348] *Ibid*.
[349] *Ibid*.

typically a decision for the courts. However, as discussed in Chapter 3, under the *Regulation*, this is now a function of search engine operators such as Google.

Considering Google as a gatekeeper within the current community of the Internet, it is clear the role it can have on the shaping of that community. And the role of gatekeeper is further solidified by the EU's insistence that Google decides what may be removed from the Internet under the *Regulation.* The Internet has created a new environment where not only traditional news and knowledge are shared, but also it is now a surrogate community for much more personal information. As stated in Chapter 2, the proliferation of the personal information on the Internet has led to governments such as the EU attempting to regain control when that personal information is misused. It is here where Google has a direct impact on the human rights of individual users. By channeling information through its search engine, Google provides a platform for the continued dissemination of personal information and a platform for the—at times—unjustified censorship of information from the Internet. Although Google is not the creator of any of the content that is displayed through its search engine website, it allows users to navigate the Internet.[350] This navigation feature of Google is the area that is being attacked by the *Regulation*. In the event of a successful right to be forgotten claim Google does not have the ability to remove the content, but rather makes it a lot more difficult to access. Google retains this role and the power that it comes with as individuals must inevitably pass through their gate to access the Internet. As summarised by James Grimmelmann, "…the reason we think of the internet not as a chaotic wasteland, but as a vibrant, accessible place, is that some very smart

---

[350] *Supra* note 345 at 175.

people have done an exceedingly good job at organizing it…"[351]. Google's search engine website can be viewed as a critical access point to the Internet, where Google decides on the visibility of information through its page-ranking feature, making certain information more visible than other information if it is displayed near the first result. This sphere of influence Google commands aligns with the concept of CSR, where private businesses are expected to be responsible for human rights within their sphere.[352] Google must be responsible for human rights within its sphere as it shapes public opinion and facilitates democratic discourse.[353]

6.3 Moving Toward CSR Regulation

Google controls information on the Internet. While Google is different from other organizations that facilitate free expression as it does not produce content, the power of the search engine in the modern era affects democratic culture. This function of Google search, that it can have an impact on the democratic culture of society, is recognized by the *CJEU* in *Google Spain* where the Court states that search engines such as Google affect fundamental rights such as the right to privacy.[354] Unlike traditional media outlets where being a gatekeeper of information is explicit, Google is more subtle and therefore any restriction placed on the free flow of information can be arguably more dangerous.[355] However, while Google commands this crucial role for speech on the Internet, the regulation of Google—including the *Regulation*—can best be described as 'light touch'.[356] This is partly because technology is constantly changing, but also current attempts to

---

[351] *Ibid*.
[352] *Supra* note 345 at 47.
[353] *Supra* note 3.
[354] *Supra* note 11.
[355] *Supra* note 345 at 172.
[356] *Supra* note 345 at 194.

regulate Google are filled with half-baked measures. Without any guidance on how Google should deal with complaints under the *Regulation*, Google has been left to its own devices to control the flow of information through its website. The current legal framework that surrounds search engines such as Google can be described as minimal application of state laws combined with self-regulation driven by the technology industry.

The Council of Europe (an international organisation with a focus on human rights within Europe) is aware of the crucial role that search engines play on the Internet and believes that change must be made if we are to regulate effectively the search engine territory of the Internet.[357] The Council of Europe makes the following recommendations:

a) Increased transparency in the selection, ranking and removal of information;
b) Filtering and blocking of content should only take place in limited circumstances to avoid breaching human rights; and
c) Continued promotion of self- and co-regulatory framework on the Internet.[358]

These recommendations can be used to develop an additional model within the *Regulation* that can be driven both from top-down black letter law and further CSR implementation.

Although we cannot access Google's internal CSR frameworks, we can look at their Terms of Service, to see how Google regulates its 'content'. On a review of its Terms of Service, the

---

[357] *Supra* note 345 at 195.
[358] *Ibid*.

picture is—somewhat expectedly—vague and leaves a lot to be desired.[359] One striking example states that Google does not necessarily review content before it is removed from its website, and puts users on warning to assume it does not review content that may infringe the law. Such a bold claim by Google, tucked into its Terms of Service, can have serious implications if the content being removed should be protected by freedom of expression or removed because of a privacy violation. While impairing fundamental human rights with no available recourse, Google is attempting to immunise itself from liability.[360] Such high value content should not be removed without proper scrutiny and assessment of its merit. In addition, the admission by Google that is does not review content before it is removed, is somewhat troubling when contemplating the *Regulation*. As has been mentioned in Chapter 3, the *CJEU* did not provide Google in *Google Spain* with any guidance as to how to complete a right to be forgotten assessment. While it may be foolish to assume that Google would continue its practice of not reviewing content applicable to the *Regulation*, such behaviour paints a bleak picture for any hope that the *Regulation* would be carefully implemented into search engines operators' business practice.

A call for transparency in Google's internal review of content is overdue. Such a recommendation, as noted by the Council of Europe, is equally applicable to Google's business-as-usual reviews of content as well as a request subject to the *Regulation*. Transparency is not only needed but expected by society when there is a risk that human rights might be impaired.

---

[359] Google, "Google Terms of Service" (14 April 2014), *Google Privacy & Terms* (website), online: <https://www.google.com/policies/terms/>.
[360] *Supra* note 345 at 215.

Google must be given some credit in relation to this point as it currently does communicate with users that content has been removed due to legal restrictions.[361] Credit must be given as this—among many other things—is an example where the *Working Party* and Google are at odds. As was discussed in Chapter 3, the *Working Party* does not believe that such communication is necessary and explicitly states this in their guidance document issued following *Google Spain*. However, the removal of content without warning or without notice is extremely dangerous and amounts to censorship as information is taken out of circulation by Google. The lack of transparency exacerbates the current tension present when Google censors access to information provided through its search engine. Users of the Internet should know what and why information has been removed.

In light of this censorship taking place online, there is a strong need for a remediation process within the Internet. Currently there is no formal or informal process that deals with the removal of content online. It is important to pause on this point. There is currently nothing, outside the courtroom, to enable remediation of the infringement of human rights on the Internet. Such a statement seems shocking only if it were not reality. Western states have yet to come to any consensus on important issues such as hate speech, pornography, obscenity and privacy. Without any cohesion, society is again left with no protection in relation to impaired human rights online. Not only is there a complete lack of protection, there is also a complete lack of remediation available when content is removed by search engine operators. The different schools of thought that dominate the discussion of Internet regulation are wholly at odds. One

[361] See section 3.4.2, above, for more on this topic.

camp believes that regulation must come from within the industry alone—self-regulation[362]—, while the other camp believes that a hybrid of state-sponsored regulation and industry regulation—co-regulation[363]—is the only effective means of regulating the Internet. While it is outside the scope of this thesis to explore the theory of self- and co-regulatory on the Internet, the CSR model discussed below is an example of a co-regulatory system. As we have seen over the last decade, neither camp's theory has provided the Internet's panacea. Instead, we find the Internet—despite being a universal tool that impacts billions of individuals daily—a mess of ill-considered regulation that is rarely enforced and easily circumvented. Without any meaningful regulation from either camp, an alternative is to create a co-regulatory regime of state sponsored regulation that is implemented through internal CSR procedure and policies created by the gatekeepers to the Internet.

As mentioned above, the Council of Europe recommended two key areas of reform that need to occur within the role that search engine operators play on the Internet. Namely these are:

a) Transparency; and

b) The limitation of the removal and blocking of content.

---

[362] Jeanne Bonnici, *Self-Regulation in Cyberspace* (New York: Cambridge University Press, 2008) at 23—24 (Definition of self-regulation can be described as a control or governance structure authorised and enforced by someone other than government (local or central) that has a particular intention. Three characteristics can identify self-regulation: (1) A flexible type of regulation model; (2) A set of rules developed and accepted by those who are taking part in an activity; and (3) A regulatory process.).

[363] A definition represents the concept of self-regulation and regulation from government (local or central) working together to achieve a particular intention.

These two limbs can be used to develop a clear co-regulatory system by both the EU Parliament through legislation and the private business through CSR. In addition to the recommendation by the Council of Europe, there is a need for a sufficient remedial mechanism to be built within any CSR policy and procedure adopted by private businesses.[364] As already mentioned, when private businesses are dealing with high-value content such as the questions of privacy and freedom of expression, there is a need for any decision-making process to mirror that of a court. Currently, the complete absence of such a remedial procedure both within the *Regulation* and in search engines' instances of removal of content is disquieting.

Before outlining in more depth the CSR model proposed, it is important to mention benefits and costs of the proposed co-regulatory model.

6.3.1 Costs of Co-regulation

First, imposing further internal regulation on a private business is never going to be a popular measure and can be criticised for chilling innovation. In particular, this problem is heightened when we consider the Internet industry where many advances that are celebrated arose from the basic nature of the industry that allows small 'start-up' companies to grow rapidly free of legal burden.[365] Burdens, like the proposed CSR model, will require additional compliance by private businesses and more capital. However, the point is to disrupt the industry, in particular those who are gatekeepers.[366] The entire rationale behind the model is to re-align the behaviour of the

---

[364] *Supra* note 345 at 245.
[365] *Supra* note 345 at 242.
[366] *Ibid.*

gatekeepers with the behaviour that individuals expect when they are on the Internet, including the protection of their human rights. Further, while the model may be portrayed as drastic and oppressive, the focus is not on all players on the Internet, only those that have amassed immense power and effect participation in democratic culture.[367]

Second, co-regulation can be criticised for the comparatively little expertise a government will have when attempting to regulate an innovative industry such as the Internet. As national governments are not in the same business as Google, they are at a disadvantage in relation to assumed knowledge and therefore the regulation can come under attack for being unsuitable. Here a risk is created that if imperfect regulation is created by the state, it will be ineffective and become redundant. The current *Regulation* cannot be described as a co-regulatory approach as it has come directly from the EU Parliament making the risk of it being redundant real. In comparison, the CSR model can represent a relationship between the state and industry participants. While the state sets and oversees minimum benchmarks, industry participants are able to interpret and implement such benchmarks appropriately.

Finally, co-regulation is critiqued for its mandatory compliance through state enforcement. However, as we have seen to date gatekeepers have had no interest in developing their own procedure that appropriately deals with the complex environment of human rights law. Such a model, if voluntary, would only draw in those industry participants who are already committed to

---

[367] *Supra* note 345 at 243.

the protection of human rights. Those who are not interested simply would not join and the protection of fundamental rights would continue to be sidestepped on the Internet.

6.3.2 Benefits of Co-regulation

As mentioned above, as a critique, co-regulation is enforced by the state using its authority to make and implement law and regulation. Such legitimacy and enforcement is an advantage co-regulation has over self-regulation. Self-regulation, while representing exactly what the industry participants desire has no ability to ensure enforcement. As is evident in YouTube's comments regarding infringing copyright[368], private organisations have little incentive and even less ability to assess and oversee regulation adequately, whereas this is a mandatory role of central and local governments. The Levenson Inquiry in the United Kingdom provides an illustration of how pure self-regulation fails without external governmental oversight.[369] The Inquiry found that the Press Complaints Commission (*PCC*), a self-regulatory industry watchdog, failed to provide independence adequately, remedial action and held too much power.[370] Unfortunately, no search engine operators have developed or implemented a self-regulatory framework that effectively addresses transparency, due process and the protection of fundamental values in relation to the removal of content from the Internet, leaving the top-down legislative approach as the only appropriate solution. A top-down mandatory approach will be able to sufficiently oversee a system that deals with freedom of expression and the right to privacy. If the *Regulation* wants to

[368] See section 5.2.2, above for more on this topic; See also *Supra* note 286 at 247.
[369] *Supra* note 345 at 254.
[370] *Ibid*.

remove a once judicial-only assessment to private businesses, adequate parameters must be built in to ensure those human rights are appropriately considered.

Co-regulation is a hybrid collaboration between private industry and state. Private business will attend to protection of the interests of industry participants and the state can ensure that what is in the public interest is included in any regulation of the Internet.[371] This democratic nature of co-regulation advances the protection of the fundamental human rights that private organisations overlook and those that have not been included in the *Regulation*. Input from the state helps to ensure that regulation will be procedurally fair, accountable and in the public interest. And input from private organisations alleviates the jurisdictional overreach currently envisaged by the *Working Party*, as gatekeepers implement their CSR regimes globally.

6.4 The CSR Model

The current lack of guidance by the EU in relation to the practical implementation of the right to be forgotten has led to an opaque process that threatens basic human rights. The *Regulation* must be amended to include an internal CSR model that builds in protection of those human rights and ensures that each assessment under the right to be forgotten is appropriately balanced. The CSR model discussed below could be included in an amendment to the *Regulation* and would help ensure that, with the assistance of governmental oversight, the public interest, due process, transparency, privacy and access to information are protected.

---

[371] *Supra* note 345 at 250.

The CSR model must be centred on two key elements resulting from the current lack of regulation for search engine operators. These are:

a) Top-down state regulation that builds human rights safeguards into private businesses' governance; and
b) A dispute resolution mechanism.

6.4.1 State Regulation Protection

As mentioned above, the content that passes through the gate that search engines keep can be considered worthy of protection of human rights such as freedom of expression and the right to privacy. The CSR model must have built-in protection to ensure that gatekeeping is procedurally fair, accountable and in the public interest.[372] Such regulation from the state could be incorporated into the *Regulation* and provide for the necessary minimum level of protection to be adopted by each search engine operator. By incorporating human rights protection into the *Regulation* and requiring private businesses to have increased regulation, new protection for individuals who have been harmed by content that has been displayed or removed by search engine operators becomes available. While the *Regulation* explicitly mentions that human rights, such as the right to privacy,[373] must be considered under a right to be forgotten request, there is no practical guidance as to how such a consideration should take place. A model that regulates how requests under the *Regulation* are considered will be a huge step in the right direction.

---

[372] *Ibid*.
[373] *Supra* note 4 at 44, see art 17.

With government setting the tone for human rights protection within the governance of private businesses, there is a greater chance of compliance as regulating the gatekeeper determines all that must pass through the gate, in the case of Google, being the 1.17 billion users it allows to pass through its gate each month. As discussed above, the legislative framework must include elements from the judicial system that promote due process, fair procedure and accountability. For example, the CSR model would include a defined transparent procedure for all complaints or assessments of content that are subject to the *Regulation*. Currently, the procedure can be best described as opaque with no information provided on how Google, or other search engines, decide each individual complaint. Providing publicly accessible anonymized case summaries of decisions is not novel and is common practice in many privacy and human rights commissions within Western society and is completed without further intrusions on individuals' privacy. What is novel is regulating that search engine operators produce such publications. Such case summaries could even be incorporated into annual reports published by search engine operators. It is here where the CSR model displays its flexibility as search engine operators while regulated to provide publicly accessible summaries of each right to be forgotten application can choose how to provide such summaries to the public.

Finally, legislated rules must be incorporated into the CSR model to ensure that any assessment undertaken in the CSR model follows appropriate rules of conduct.[374] If we are—and the right to be forgotten is—going to move adjudication into the hands of private businesses there must be a

---

[374] *Supra* note 345 at 257.

code of conduct that enables such organizations to meet this role. To ensure that compliance can be as easy as possible, any rules must represent due process and also be predictable, accessible, transparent and proportionate.[375] At a minimum the following rules would be included in the CSR model that is proposed as an amendment to the *Regulation:* Every request in relation to the right to be forgotten must:

a) be assessed within 30 working days, in the event that additional time is needed, this must be communicated to the requestor as soon as practicable;
b) be assessed consistently with the due process, fairness and accountability;
c) be considered in light of all of the following:
    i. the individual's right to privacy,
    ii. the public interest,
    iii. freedom of information, and
    iv. freedom of expression;
d) have a dispute resolution procedure available; and
e) in the case of a successful application, be effectively communicated on the search engine website that content has been removed.

The above rules are provided as a starting point and are not exhaustive. They highlight, briefly, what the right to be forgotten risks ignoring and will assist private businesses with their internal assessment of individual right to be forgotten requests.

---

[375] *Supra* note 345 at 258.

Further, there must be education offered to both the public and those private businesses that would be subject to the rules. For example, the due diligence of a private business when assessing a request would have such rules built into its internal procedure ensuring that all appropriate measures have been considered.

Legislative regulation can be portrayed as a blunt tool to curtail bad behaviour and stifle innovation. However, the proposed CSR model described here is not blunt but simply provides a regulated backdrop within which private businesses can develop their own rule of governance. By ensuring that certain minimum standards are in place within the *Regulation*, individuals not only receive better access and understanding as to how search engine operators decide their requests, but also have some assurance that their human rights are considered adequately in the process.

6.4.2 Dispute Resolution Procedure

The complete absence of any right of reply or ability to challenge the decisions made by private businesses in relation to the regulation of content on the Internet is shocking. Similarly shocking is its absence from the *Regulation.* As discussed, search engine operators are gatekeepers of information that passes through their websites. If certain content is removed by such gatekeepers, the affected individual and the content has been removed from participating in the democratic discourse found on the Internet.[376] The availability of a dispute resolution

[376] *Supra* note 345 at 261.

mechanism to challenge the decision of search engine operators allows individuals participation in the democratic discourse.

The dispute resolution mechanism proposed has the ability to become an extremely active area for search engine operators when considering the volume of users that are channelled through search engines. This begs the question whether an independent body is needed to facilitate such claims or whether private businesses can absorb the cost entirely. While the cost of such a mechanism is beyond the scope of this thesis, it is worthy to consider. Funding could occur through mandatory membership fees or an administrative fee levied on each dispute payable by the individual. An individual dispute fee would also help prevent litigious and vexatious individuals from clogging the dispute resolution mechanism. Although the purpose of this Chapter is not to provide a descriptive account of the mechanics of such a procedure, Emily Laidlaw has developed a robust set of principles that can guide such procedures. Her principles—in chronological order—are:

a) Complaints are assessed as to whether or not they meet the threshold for the dispute resolution procedure;
b) After passing the threshold, the complainant and the private business can be offered mediation to resolve the complaint;
c) If mediation is not pursued, the complaint will be assessed by the dispute resolution committee allowing both the complainant and the private business to submit their representations; and

d) The dispute resolution committee makes a decision and may impose a pecuniary penalty or other relief.[377]

The above set of principles cannot be described as offering an alternative as currently there is no similar procedure in place in relation to search engine operators. The implementation of a dispute resolution procedure fills a glaring gap in the current *Regulation* and attempts to level the playing field for individuals and private businesses.

The CSR model described in this Chapter is a co-regulatory model that will further the protection of human rights in an industry that has a dubious history of the protection of such rights. The legislative framework provides a concrete foundation and necessary oversight that society expects from the state and ensures that minimum standards are not only met but which are systemic in any internal governance procedure. It also provides industry participants with flexibility as they can interpret and implement the rules in the most appropriate format for each private business. This flexibility enables industry participants to cater the formality of their dispute resolution procedure to their circumstances including size and financial resources. Again, the co-regulatory model approaches flexibility to ensure that all are not painted with the same brush and administrative costs are aligned with capabilities of each industry participant. Laidlaw provides an outline of how such a procedure could work, illustrated in figure 6-1 below.

---

[377] *Supra* note 345 at 265.

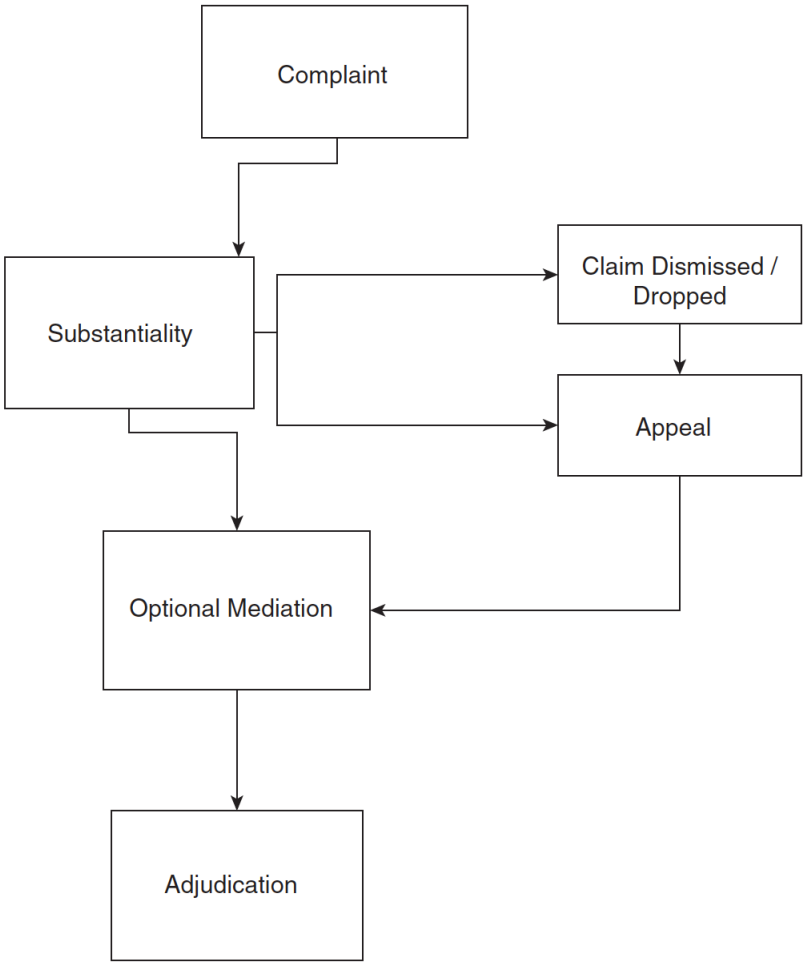

Figure 6-1 Remedial Process[378]

Figure 6-1 provides one possible format of a dispute resolution procedure that could be adopted by industry participants if the *Regulation* is amended to include the CSR model. The following provides a brief explanation of each action in figure 6-1:

[378] Figure 6-1 from © Emily B Laidlaw, *Regulating Speech in Cyberspace Gatekeepers, Human Rights and Corporate Responsibility,* (United Kingdom: Cambridge University Press, 2015), at 266. By permission from the author.

1 A complaint is made by an individual in relation to their right to be forgotten request. This step can be designed in multiple formats to ensure that only serious complaints are made. This action could be designed to be time and fact sensitive to ensure that only legitimate complaints are submitted;[379]

2 The substantiality action will require reasonable investigations to be made by the industry participant to ensure that no vexatious or trivial claims are submitted through the dispute resolution procedure. Complaints that meet this threshold would be submitted to mediation. Complaints that do not meet this investigation can be dismissed and no further action would be required by the industry participant;

3 A complainant has the option to appeal the outcome of the suitability assessment and proceed to mediation. The availability of an appeal allows serious complainants to pursue their complaint and ensures that they have the opportunity to be heard at mediation;

4 Mediation may take place between the parties if consented to by mutual agreement. If the complaint cannot be resolved by mediation, the complaint proceeds to adjudication by an oversight body; and

5 Adjudication by an oversight body occurs where such a body has the ability to award damages and/or corrective action.[380]

As stated above, the above figure 6-1 and discussion highlights one possible format of dispute resolution possible under the CSR model, that would provide transparency and protection of fundamental human rights within the *Regulation*.

---

[379] *Supra* note 345 at 262.
[380] *Ibid* at 260-263.

6.5 A Reasonable Expectation of Privacy

As discussed above, the scope of Article 17 is extremely wide because of the broad definition of personal data[381] combined with the absence of any qualifications that have become customary within privacy theory. Personal data, under Article 17, relates to any identifiable information about an individual which on its own is unremarkable in privacy discourse. However, within privacy discourse such definitions typically are quickly followed with a qualification that the individual had a reasonable expectation of privacy over that personal data before a remedy will be granted. Article 17 does not go this far, leaving the door wide open for Article 17 to be used in instances where there has never been an expectation of privacy, if the request is accepted by a data controller (search engine operator), it will be 'forgotten'. The introduction of a reasonable expectation of privacy to Article 17 would be straight-forward and could be stated as follows:

> 1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her, **where the data subject had a reasonable expectation of privacy**, and the controller shall have the obligation to erase the personal data without undue delay where one of the following grounds applies…

Including a reasonable expectation of privacy assessment within Article 17 would narrow the scope of abuse that Article 17 could face with such an open definition of personal information and help align and protect privacy expectations. Further, a definition of 'reasonable expectation

---

[381] *Supra* note 4 at 33, see art 4.

of privacy' would need to be included within the *Regulation*. The next section within this Chapter will explore what such a definition could look like.

6.5.1 A Reasonable Expectation of Privacy on the Internet

The two-pronged test, briefly mentioned in Chapter 4, developed in *Katz*[382], requires an assessment of both the objective and subjective factors that centre around an intrusion of privacy claim. Due to the wide adoption of this test outside of the US[383], an individual must prove both that there had been a subjective reasonable expectation of privacy on behalf of the individual and that the facts point toward an objective reasonable expectation of privacy. Without both elements being established, courts are unable to conclude that a reasonable expectation of privacy existed resulting in the absence of a privacy intrusion worthy of redress. It must be noted that the decision in *Katz* was made in 1967 and while the assessment has been contoured by courtrooms across the world, the foundations of the subjective and objective elements remain. These foundations have served courtrooms greatly since 1967 and helped establish a sphere of protection offered by the courts when privacy is intruded upon. However, the Internet age has drastically changed individuals' expectations of privacy in so much that the objective test developed in *Katz* has become unfit for its purpose.[384]

The current pace that the Internet advances and changes direction has left regulation constantly playing catch-up. The reasonable expectation of privacy test is another casualty in this constant

---

[382] *Supra* note 255.
[383] *Supra* note 259; *Supra* note 119.
[384] *Supra* note 297 at 343—344.

game of catch-up. As the digital environment progresses, the area in which the reasonable expectation can be established has been diminishing.[385] Rather than allow the Internet to dictate where privacy can be established, there is a need to redefine the reasonable expectation of privacy so it can be established on the Internet. The primary failure of the current assessment of a reasonable expectation of privacy can be found in the subjective and objective expectations of privacy found on the Internet.[386] The increasing pervasiveness of the Internet and extremely high penetration has led to a gap between what courts assess as being private and what an individual perceives as private.[387] As the Internet is seen as an open platform for democratic discourse, among others, objectively it is easy to establish that the Internet is a public place and therefore cannot attract a reasonable expectation of privacy. This problem is strengthened when courts look to the underlying technology as a guide to how privacy should be examined. While the Internet may seem to not attract privacy objectively, individuals expect a reasonable level of privacy. This lack of objective privacy is easy to understand as Internet users, particularly individuals that grew up with the Internet, share more information on the Internet than ever.[388] Social validation can be achieved through the amount of likes or shares a post receives on SNWs such as Facebook. Achieving the largest audience possible through SNWs is promoted and encouraged on the Internet. These attributes often leave a court with nowhere else to turn besides finding that there can be no reasonable expectation of privacy. However, it is important

---

[385] *Supra* note 297 at 344.
[386] *Supra* note 297 at 345.
[387] *Supra* note 297 at 351.
[388] *Supra* note 297 at 352.

to question this philosophy as, despite the action of overzealous sharing, individuals still expect some privacy on the Internet.

Article 17 of the *Regulation* was introduced as a protector of privacy, however, as this thesis has highlighted it comes with many flaws and furthers the divide between the objective and subjective expectations of privacy. With such a wide scope in the current draft, privacy is no longer being protected but rather Article 17 can be seen as diminishing privacy and furthering censorship. Introducing a new reasonable expectation of privacy that aligns with how individuals perceive their privacy on the Internet will prevent drastic censorship while sustaining the value of privacy to both individuals and society.

The new reformed reasonable expectation of privacy must move away from technology dictating what and where are private and shift toward how individuals view their privacy. As mentioned above, although many users on the Internet are quick to share information on the Internet, this does not equate to a total lack of a reasonable expectation of privacy. The first step of the two-pronged test developed in *Katz* (then adopted in *Tessling*) needs to be replaced with a societal expectation of privacy rather than an objective assessment.[389] While individuals recognize that the Internet provides an open platform for speech, sharing and expression, there remains an expectation of privacy within the Internet.[390] Rather than looking simply at whether the Internet can harbour an objective reasonable expectation of privacy, like a court does, individuals look to

---

[389] *Supra* note 297 at 364.
[390] Valerie Steeves, "If the Supreme Court Were on Facebook: Evaluating the Reasonable Expectation of Privacy Test from a Social Perspective" (2008) Canadian J Criminology & Criminal Justice 50:3 at 339.

the particular space and context to determine their expectation of privacy.[391] The six step test developed in *Tessling* provides a good example of how the current assessment does not match social expectation of privacy. The assessment in *Tessling* disregards societal context and therefore does not align with how users of the Internet actually perceive their expectations of privacy.[392] For example, the first element of the test in *Tessling* considers the place and subject matter of the intrusion. From the perspective of an Internet user, examining the place where the information was shared is almost redundant. Mobile technology has changed the ability of individuals to use the Internet allowing private communications to take place virtually anywhere with a connection to the Internet. To limit the assessment to a physical location removes the consideration of the individuals' expectation in place of focussing on where the communication took place.[393] The place will most likely be irrelevant to the individual as the pervasiveness of the Internet does not mean that individuals adapt their online behaviour because of the physical space they are in. Further, the second assessment in the *Tessling* test considers whether the information is in the public view. This assessment is also problematic when relating it to activities of individuals on the Internet. Although there is a great understanding of the ease with which emails and instant messaging services can be exploited, those who use such applications still desire and expect a level of privacy. In addition, the Internet is a fundamentally open space and therefore applying *Tessling*, it is easy to establish that large amounts of information cannot be deemed private. Making this conclusion ignores the expectation of the individuals using these

---

[391] *Ibid*.
[392] *Supra* note 390 at 343.
[393] *Supra* note 390 at 340.

services. Social expectation reveals that individuals treat their computers and mobile devices more privately than courts expect.[394]

Removing the objective requirement adopted in Canada in *Tessling* will enable the reasonable expectation of privacy assessment to align with the actual expectations individuals have in relation to their behaviour on the Internet. Incorporating a social expectation of privacy will not risk privacy protection becoming too accessible as the assessment still requires an expectation of privacy to exist. In order to assess the social expectation of privacy, courts—and search engine operators in accordance with a reformed Article 17—should adopt an empirical approach to determine social expectations of privacy on the Internet.[395] This approach would create a standard where privacy expectations expected by individuals align with protection offered by the law. Such empirical measurements could be in the format of a survey where certain activities relating to privacy and surveillance are ranked between 1 – 10. It should be noted that undertaking empirical research for each individual case would be a huge administrative cost to a court or a search engine operator. However, this would be somewhat alleviated by the fact that independent research could be driven by courts embracing empirical research within their assessment. In relation to the likes of Google, independent research could also arise from the search engine pursuing such research. Further, the scope of empirical studies undertaken by search engine operators could be significantly narrower than a court's. Search engine operators would only have to ensure that any empirical studies covered the activity governed by Article 17.

---

[394] *Ibid*.
[395] *Supra* note 297 at 364.

While this would still require significant cost, the current statistics of Article 17 requests highlight a few key areas of behaviour that individuals believe the right to be forgotten applies to. According to Google's Transparency Report SNWs have accounted for 8 of the top 10 websites requested to be removed by individuals.[396] This trend would allow any empirical research undertaken by search engine operators to be more focused and therefore lower in cost. The reformation of the test adopted in *Tessling* would narrow the discretion that judges and Google employees have currently when assessing an individuals' privacy. Narrowing this discretion toward what is actually expected by individuals will create a more accurate understanding of privacy on the Internet.

Including the reformed reasonable expectation of privacy test into Article 17 will be a step toward regaining control of privacy in the high speed growth of technology. Without a reasonable expectation of privacy considered within Article 17, access to so-called privacy protection will go unwatched, leading to both unfounded censorship in the case where information that should not attract privacy protection is granted such protection and to an erosion of what privacy represents on the Internet where technology determines privacy rather than the individual.

---

[396] *Supra* note 78.

Chapter 7: Conclusion

The Internet occupies unique territory within society. It does not exist in only one space or one format but affects countless individuals. Similar to social understandings of privacy, the Internet can take on vastly different meanings and be used in vastly different ways depending on the context. It can be used as a business tool, a surrogate for community and a place to exchange and communicate personal information. However simply because all of these activities occur through the technology that represents the Internet, does not mean they should be all regulated under the same approach. Article 17 of the *Regulation* treats all personal information on the Internet as if it were the same without exploring the privacy expectations associated with that information. Beyond the *Regulation* being only a partial solution to current privacy intrusions on the Internet, the EU has fallen short of any meaningful guidance on how private businesses should implement the drastic step of removing information from the Internet.

As discussed throughout this thesis, the right to be forgotten as currently drafted in the *Regulation* does not provide an appropriate solution to unauthorized disclosure of personal information on the Internet. Although it does offer a solution, it is not perfect and creates risks for the democratic nature of the Internet and the continued protection of privacy and freedom of expression. Rather than attempt to alleviate the cause of unauthorized disclosure online, Article 17 simply will treat the symptoms only. The Internet has been a part of Western society for nearly 3 decades yet little coherent regulation is in force globally that addresses privacy while protecting freedom of expression. Unfortunately, the *Regulation* continues this trend and to be effective must be amended.

The current drafting of the *Regulation* will lead to an Internet environment where fundamental values that were once assessed and considered within the courtroom will be decided behind closed doors of private organisations. While it is important to acknowledge that the immense traffic[397] and scope for complaints on the Internet highlight that a movement away from the courtroom is efficient, such a move must be cautiously exercised. The lack of valuable guidance from the EU does not equate to a cautious move away from the courtroom. It is more akin to a leap in the dark. The study of privacy is extremely nuanced and can take on different meanings dependent on social context and the expectations present within society. This thesis outlined three theories as to why individuals and society value privacy. Each theory related to the control of oneself and their personal information. All three theories all outlined that privacy was a contextual analysis that can be viewed entirely differently dependent on that context.

The current drafting of Article 17 and the *Regulation* does not place enough emphasis on the contextual analysis of a request under Article 17. The *Regulation* does state that any request must be considered within the scope of other law including the right to freedom of expression. This consideration is important and ensures that search engine operators at least consider other important values. However, Article 17 is drafted too widely allowing any individual who has personal information on the Internet to be subject to Article 17. Such a wide definition of personal information is not uncommon, but the absence of any other qualifications is. The well-known reasonable expectation of privacy assessment should be included in an amendment to the

---

[397] *Supra* note 343 (Google receives 1.17 billion unique views monthly).

Regulation to ensure that the contextual elements of an individual's privacy are considered. A reasonable expectation of privacy assessment would provide Article 17 with an appropriate and all-encompassing consideration that is needed to temper the risk of corporate censorship and overbearing jurisdictional reach. As highlighted in this thesis, the potential risks with the *Regulation*, and in particular Article 17, are censorship, devaluing privacy and the futility of enforcement resulting from circumvention beyond the jurisdictional reach of the EU.

These concerns cannot be overlooked. The *Regulation* governs the gatekeepers of the Internet, yet the *Regulation* cannot achieve the desired effect and in doing so will risk censoring the open Internet that western society has come to celebrate. The risk of censorship is further increased by the guidance of the *Working Party* that recommends no publicity for Article 17 requests that are approved. As already mentioned, this is an unacceptable position on the Internet where information will disappear without any ability of individuals to find out why the information has been removed. Further, heading down the censorship path is dangerous looking to the example of China. In China, censorship is widespread on the Internet and stems from the mundane to the extreme.[398] An Internet that is not only censored but also opaque is not an open Internet and is a real risk under the *Regulation*. Aligning social expectations of privacy with regulation of the Internet promotes a workable and valuable definition of privacy currently lacking in the *Regulation*. The jurisdictional dilemma faced by the right to be forgotten highlights the disconnect across the globe as to how best to regulate the Internet. Without global implementation of the successful right to be forgotten requests, Article 17 becomes futile. It is

[398] See section 5.2.1, *above*, for a discussion on this topic.

already known that Google is not willing to comply with the worldwide implementation of Article 17 allowing circumvention of any Article 17 request with a few keystrokes. Global implementation in relation to jurisdiction on the Internet is an important consideration for any regulation created specifically for the Internet. As is currently being seen in the appeal of *Equustek*[399], the Supreme Court of Canada will soon decide on whether such orders are acceptable within Canada. The decision in *Equustek*[400] will be of vital significance to the future of Internet jurisdiction cases within Canada.

The highlighted problems of censorship, devaluing privacy and jurisdiction can be tempered by the amendments proposed in this thesis. First, the inclusion of a CSR model within the *Regulation* would ensure that the procedure for removal of information from the Internet was exercised with fundamental human rights and proper procedure at the forefront of private businesses' assessment. Private businesses do not have best history when it comes to the removal of content from the Internet, with both YouTube and Google seemingly happy to not review content before it is removed.[401] The severe financial penalties that exist in the *Regulation* incentivize this behavior. However, the thorough CSR model that includes procedural fairness, the protection of fundamental values and a remedial process will enable private businesses to consider each Article 17 request appropriately and avoid draconian censorship. In addition, the CSR model will introduce much needed transparency by ensuring that the outcomes of all Article 17 requests are published and publicly available. Not only will this promote transparency but

---

[399] *Supra* note 244.
[400] *Ibid*.
[401] See section 5.2.2, above for more on this topic.

also education as individuals will be able to assess their request in light of the published precedents. The CSR model is a movement toward co-regulation on the Internet that can prevent the current ease of circumvention that exists under the *Regulation*. As the CSR model shares the responsibility of regulation with both government and private businesses, there is a higher likelihood of buy-in from private businesses. Not only does this benefit the effectiveness of regulation, as it is more likely to be enforced with participation from those who it affects, but it opens up cross-border enforcement as global companies such as Google adopt the CSR model. The CSR model can offer the *Regulation* much needed transparency as well as critical endorsement from industry participants. The current divergence between Google and the *Working Party* diminishes the effectiveness of the *Regulation* and risks seeing it abandoned.

Second, the introduction of a reasonable expectation of privacy assessment into Article 17 will prevent improper use of the *Regulation* and re-align it with societal expectations of privacy. The current wide drafting of Article 17 and the definitions found in the *Regulation* leave the door wide open for inappropriate use of Article 17. Because Article 17 attempts to cast such a wide net it creates a risk of censorship on the Internet where personal information that does not attract a reasonable expectation of privacy may be removed from the results of search engine operators and become forgotten on the Internet. Amending the *Regulation* to include a reasonable expectation of privacy would align with the current understanding of privacy within the jurisdictions examined in this thesis. The assessment is now unexceptional in courtroom analysis making for an easy introduction into the *Regulation.* While the current assessment of a reasonable expectation of privacy is unexceptional, this thesis proposed re-shaping the assessment in a post-Internet world. The reasonable expectation of privacy proposed here should

allow for the social expectation of privacy to be considered in place of the current objective assessment. The Internet represents a place that is so varied, it is unfair to consider only whether privacy can be expected on the Internet from an objective perspective that looks heavily to the Internet's technological foundations. While the Internet, objectively, might be the last place an individual can find privacy, there is a growing societal expectation that it does exist on the Internet. Recognition of this expectation will align the *Regulation* with how the Internet is used by individuals. Such alignment is beneficial as it enables the *Regulation* to be used appropriately while cementing a more accurate protection of privacy on the Internet.

The right to be forgotten as currently drafted within the *Regulation* highlights the need for further protection of personal information on the Internet. It also highlights the disconnect that currently exists between government regulation, industry participants and individuals. The end goal of the right to be forgotten is a step toward claiming back some control over the Internet, but comes at a cost. The Internet is one of most universally celebrated technologies of modern history and must continue to be celebrated without being burdened by the risk of censorship or the futility of regulation that cannot be enforced. Amending the *Regulation* to ensure transparency exists to protect fundamental human rights and to ensure that it aligns with societal expectations of privacy is something worth remembering.

Bibliography

LEGISLATION

CANADA

An Act Respecting the Protection of Personal Information in the Private Sector, CQLR 1993, c P-39.1.

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

Charter of Rights and Freedoms, CQLR, c-12.

Personal Health Information Protection Act, SO 2004, c 3.

Personal Information Protection Act, SBC 2003, c 63.

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

Privacy Act, RSBC 1996, c 373.

EUROPEAN UNION

EC, *Commission Regulation (EU) 679/2016 of the European Parliament and of the Council of 27 April 2016 on the protection of natural person with regard to the processing of personal data on the free movement of such data, and repealing Regulation 95/46/EC (General Data Protection Regulation),* OJ, L 119/1.

EC, *Regulation 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] OJ, L 281/31.

NEW ZEALAND

New Zealand Bill of Rights Act 1990 (NZ), 1990/109.

Criminal Records (Clean Slate) Act 2004 (NZ), 2004/36.

Privacy Act 1993 (NZ), 1993/28.

UNITED STATES

The Digital Millennium Copyright Act, 17 USC § 512 1998.

JURISPRUDENCE

CANADA

A T v L T H, 2006 BCSC 1689.

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

Equustek Solutions Inc v Jack, 2015 BCCA 265, [2015] 11 WWR 45.

Jones v Tsige, 2012 ONCA 32, 251 CRR (2d) 124.

Jones v Tsige, 2011 ONSC 1475, 199 ACWS (3d) 1367.

Nesbitt v Neufeld, 2010 BCSC 1605

Niemela v Malamas, 2015 BCSC 1024.

R v Tessling, 2004 SCC 67, [2004] 3 SCR 432.

SOCAN v Canadian Association of Internet Providers, 2004 SCC 45, 32 CPR (4th) 1.

EUROPEAN UNION

Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, ECLI:EU:C:2014:317, [2014] ECR I-00000.

In re Lindqvist, Case C-101/01, [2003] ECR I-12971.

NEW ZEALAND

Brooker v Police, [2007] NZSC 30, [2007] 3 NZLR 91.

C v Holland, [2012] NZHC 2155, [2012] 3 NZLR 672.

Hosking v Runting, [2004] NZCA 34, [2005] 1 NZLR 1.

Rogers v TVNZ, [2007] NZSC 91.

Tucker v News Media Ownership Ltd, [1986] 2 NZLR 716 (HC).

AUSTRALIA

Dow Jones & Company Inc v Gutnick, [2002] HCA 56.

UNITED STATES

Katz v United States, 389 US 347 (1967).

Yahoo! Inc v La Ligue Contre Le Racisme Et L'Antisemitisme, 433 F3d 1199 (9th Cir 2006).

Zippo Mfg. Co. v Zippo Dot Com Inc, 925 F Supp 119 (WD PA 1997).

SECONDARY MATERIALS: ARTICLES

Alder, Julie. "The Public's Burden in a Digital Age: Pressures on Intermediaries and the Privatization of Internet Censorship" (2008) 20 JL & Pol'y 231.

Allen, Adria. "Internet Jurisdiction Today" (2001) 22:1 Nw J Intl L & Bus 69.

Ambrose, Meg Leta. "It's About Time: Privacy, Information Life Cycles, and the Right to be Forgotten" (2013) 16 Stan Tech L Rev 369.

Ausloos, Jef. "The 'Right to be Forgotten' – Worth Remembering?", (2012) 28:2 Computer L & Security Rev 143.

Austin, Lisa M. "Privacy and the question of Technology" (2003) 22:2 McGill LJ 167.

Bauml, Jessica E. "It's a Mad, Mad Internet: Globalization and the Challenges Presented by Internet Censorship" (2011) 63:3 Fed Comm LJ 697.

Bensen, Tierney, Patrick Henze & Geoff Farnsworth. "The Great Chinese Firewall: A Safegaurd or Stop Sign?" (2006) 2:3 Journal of Information Privacy & Security 42.

Cohen-Almagor, Raphael. “Internet Architecture, freedom of expression and social responsibility: critical realism and proposals for a better future” (2015) 28:2 Innovation: The European J of Social Science Research 147.

Crowther, Brandon. “(Un)reasonable Expectation of Digital Privacy” (2012) 1 BYU L Rev 343.

Van Alsenoy, Brendan & Marieke, Koekkoek. “Internet and jurisdiction after Google Spain: the extraterritorial reach of the ‘right to be delisted’” (2015) 5:2 Intl Data Privacy L 105.

Fish, Eric. “Internet Censorship and Democracy in South Korea” (2009) 2 Asia-Pacific Journal on Human Rights and the Law 43.

Human Rights Watch, “Race to the Bottom; Corporate Complicity in Chinese Internet Censorship” (2006) Human Rights Watch Report 18:8.

Khondker, Habibul Haque. “Role of New Media in the Arab Spring” (2011) 8:5 Globalizations 675 at 677.

Larson, Robert G. “Forgetting the First Amendment: How Obscurity Based Privacy and a Right to Be Forgotten Are Incompatible with Free Speech” (2013) 18:1 Comm L & Pol’y 91.

Lenatti, Chuck. “Tim O’Reilly and Web 2.0” (2007) 7:22 The Seybold Report: Analyzing Publishing Technologies 13.

Nolan, Justine M. “The China Dilemma: Internet censorship and corporate responsibility.” (2009) 4:1 Asian Journal of Comparative Law Article 3.

Rothschild, Max. “Corporate Cyber-Censorship: The Problems with Freedom of Expression Online” (2013) 11 CJLT 143.

Nunziato, Dawn C. “How (Not) to Censor: Procedural First Amendment Values and Internet Censorship Worldwide” (2011) 42:4 Geo J Int’l L 1123.

Pensky, Marc. “Digital Natives, Digital Immigrants Part 1” (2001) 9:5 On the Horizon.

Prosser, William. “Privacy”, Cal L Rev 48:3 (1960) 383.

Recent Cases, "Internet Law – Protection of Personal Data – Court of Justice of the European Union Creates Presumption That Google Must Remove Links to Personal Data Upon Request – Case c-131/12, Google Spain SL v Agencia Espanola de Proteccion de Datos (May 13, 2014)" Harv L Rev 128 (2014) 735.

Rosen, Jeffrey. "The Right to be Forgotten", (2012) 64 Stan L Rev Online 88.

Schultz, Thomas. "Carving up the Internet" (2008) 19:4 European J Intl L 799.

Shoor, Adams Emily. *"*Narrowing the right to be forgotten: Why the European Union needs to amend the Proposed Date Protection Regulation*"* (2014) 39 Brook J Intl L 487.

Steeves, Valerie. "If the Supreme Court Were on Facebook: Evaluating the Reasonable Expectation of Privacy Test from a Social Perspective" (2008) Canadian J Criminology & Criminal Justice 50:3.

Tsesis, Alexander. "The right to erasure: privacy, data brokers, and the indefinite retention of Data" (2014) 49 Wake Forest L Rev 433.

Urban, Jennifer M. & Laura, Quilter. "Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act" (2006) 22 Santa Clara Comp & High Tech LJ 621.

Warren, Samuel & Louis, Brandeis. "The Right to Privacy" (1890) 4:5 Harv L Rev 193.

Wolfsfeld, Gadi. "Social Media and the Arab Spring: Politics Comes First" (2013) 18:2 The International Journal of Press/Politics 115.

Xanthoulis, Napoleon. "The right to oblivion in the information age: a human-rights based approach" (2013) 10 China Business Rev 84.

SECONDARY MATERIALS: BOOKS

Bonnici, Jeanne. *Self-Regulation in Cyberspace* (New York: Cambridge University Press, 2008).

DeCew, Wagner, Judith. *In Pursuit of Privacy: Law, Ethics, and the rise of Technology* (Ithaca: Cornell University Press, 1997).

Ghezzi, A, A G Pereira & L Vesnic-Alujevic (eds), *The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten* (England: Palgrave Macmillan, 2014).

Laidlaw, Emily B. *Regulating Speech in Cyberspace Gatekeepers, Human Rights and Corporate Responsibility* (United Kingdom: Cambridge University Press, 2015).

Levmore, Saul. & Martha C. Nussbaum (eds), *The Offensive Internet: Speech, privacy and reputation* (Cambridge: Harvard University Press, 2010).

Lim, Fin, Yeen. *Cyberspace Law Commentaries and Material* (Melbourne: Oxford University Press, 2002).

Moore, Adam. *Privacy Rights: Moral and Legal Foundations* (United States of America: The Pennsylvania State University Press, 2010).

Orwell, George. *1984* (New York: Plume, 1949).

Penk, Stephen & Rosemary Tobin. (eds), *Privacy Law in New Zealand* (Wellington: Brookers, 2010).

Rössler, Beate. *The Value of Privacy* (Cambridge: Polity Press, 2005).

Rustad, Michael L. & Thomas F Lambert Jr, *Global Internet law in a nutshell,* 2nd ed (Minneapolis: West Academic Publishing, 2013).

———. *Internet Law in nutshell,* 2nd ed (United States of America: Thomson Reuters, 2009).

Solove, Daniel J. *Understanding Privacy* (London, England: Harvard University Press, 2008).

Street, Lawrence F. & M P Grant, *Law of the Internet,* 2000 Edition (Virginia: Lexis Law Publishing, 2000)

Westin, F. A. *Privacy and Freedom* (New York: Antheneum, 1967).

Zittrain, Jonathan L. *Future of the Internet and How to Stop It* (United States of America: Yale University Press, 2008).

SECONDARY MATERIALS: GOVERNMENT PUBLICATIONS

Canada, Privacy Commissioner of Canada, *Learning from a Decade of Experience: Quebec's Private Sector Privacy Act*, (Ottawa, Privacy Commissioner of Canada, 2005).

EC, Commission, *Article 29 Data Protection Working Party 14/EN WP 225 "Guidelines on the Implementation of the Court of Justice of the European Union Judgment on 'Google Spain and Inc. V. Agencia Espanaola De Proteccion De Datos (AEPD) and Marios Costeja Gonzalez" C-131/12* (Brussels: EC, 2014).

EC, *Opinion 3/2015 (with addendum) Europe's big opportunity EDPS recommendation on the EU's options for data protection reform*, Opinion 3/2015.

EC, *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age*, (Munich: EC, 2012).

SECONDARY MATERIALS: ONLINE MATERIALS

Alexa, "The Top 500 Websites on the Web", *Alexa* (website) online: < http://www.alexa.com/topsites> (retrieved 16 January 2016).

Alphabet Investor Relations, Press Release, "Alphabet Announces Fourth Quarter and Fiscal Year 2015 Results" (1 February 2016), online: <https://abc.xyz/investor/news/earnings/2015/Q4_google_earnings/index.html> (retrieved 22 June 2016).

Brown, Chris. "Flight MH370 gets crowdsourced help from scientists", *CBC News* (March 9 2015), online: < http://www.cbc.ca/news/technology/flight-mh370-search-gets-crowdsourced-help-from-scientists-1.2987450 > (retrieved 4 February 2016).

Burgess, Guy. "Name suppression and the internet" (16 November 2009), *Law and technology* (blog), online: < http://www.burgess.co.nz/name-suppression-and-the-internet/> (retrieved 6 December 2015).

Facebook, “Facebook Data Policy – How can I manage or delete information about me” (30 January 2015), *Facebook* (website), online:< https://www.facebook.com/policy.php> (retrieved 14 March 2016).

Facebook, Media Release, “One Billion People on Facebook” (4 October 2012), online: < http://newsroom.fb.com/news/2012/10/one-billion-people-on-facebook/> (retrieved 18 November 2015).

Gantz, John. & David Reinsel. “Extracting Value from Chaos” (June 2011), *IDC iView* (website), online: < https://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf >.

Google, “Are you removing pages wholesale from your search results?”, *Google Transparency Report* (website), online: <https://www.google.com/transparencyreport/removals/europeprivacy/faq/?hl=en#are_you_removin> (retrieved 22 January 2016).

Google, “European privacy requests for search removals” (24 July 2016), *Google Transparency Report* (website), online: <http://www.google.com/transparencyreport/removals/europeprivacy/?hl=en> (retrieved 8 May 2016).

Google, “Google Terms of Service” (14 April 2014), *Google Privacy & Terms* (website), online: <https://www.google.com/policies/terms/> (retrieved 5 May 2016).

Google Search, “Mario Gonzalez”, *Google* (website), online: <https://www.google.es/#q=mario+gonzalez> (retrieved 13 December 2016).

“Internet Usage Statistics: The Big Picture”, (30 November 2015), *Internet World Stats* (website) online: <http://www.internetworldstats.com/stats.htm> (retrieved 8 October 2015).

Kelly, Michael B. “China Blocks Searches for ‘Big Yellow Duck’ After Brilliant Tiananmen Square Pun” *Business Insider* (4 June 2013), online: <http://www.businessinsider.com/chinese-censors-block-big-yellow-duck-2013-6> (retrieved 1 February 2016).

Love, Jim. “Star Wars Kid” (January 15, 2006), online: YouTube <
https://www.youtube.com/watch?v=HPPj6viIBmU > (retrieved 4 November 2015).

Privacy Commissioner, “Frequently Asked Questions”, *Privacy Commissioner* (website) online:
<https://www.privacy.org.nz/your-rights/frequently-asked-questions/#fine> (retrieved 6 May 2016).