Legal Adaptation to the Internet: The Emergence of Digital Rights and Internet Personhood

by

Matthew Marinett

A thesis submitted in conformity with the requirements for the degree of Master of Laws

Faculty of Law
University of Toronto

© Copyright by Matthew Marinett 2016
Abstract

Understanding how the law has adapted to technological change in the past is critical to determining how it can best respond in the future. In attempting to do so, scholars have largely examined legal adaptation to technological change only with respect to discrete doctrinal categories. While useful, these analyses may fail to grasp the underlying human interests affected by a technology in their focus on specific areas of law. This thesis demonstrates that a holistic examination of past legal adaptations to a technology across multiple doctrinal categories helps to elucidate the underlying interests affected by a technology, and better assists in addressing challenges created by similar technologies in the future. This thesis develops a substantive theory of legal adaptation to the Internet, finding that much of the law’s response to the Internet recognizes the personhood-expanding nature of Internet use, specifically with respect to privacy, anonymity, and freedom of expression.
# Table of Contents

Introduction ................................................................................................................................. 1  

Chapter 1 Legal Adaptation to Technological Change .............................................................. 7  
1. Chapter Overview ................................................................................................................... 7  
2. A Theory of Legal Adaptation to Technological Change ...................................................... 7  
   a. What is Legal Adaptation to Technological Change? .......................................................... 7  
   b. When is Legal Adaptation Necessary? ................................................................................. 14  
   c. How Can the Law Respond to Technological Change? ....................................................... 17  
3. Why Have a Theory of Legal Adaptation to Technological Change? ................................... 19  
   a. Procedural Theories ............................................................................................................ 21  
   b. Substantive Theories .......................................................................................................... 25  
4. Why Have a Theory of Legal Adaptation to the Internet? .................................................... 28  
5. Methodology for Producing a Substantive Theory ............................................................... 32  

Chapter 2 The Internet and the Rise of Digital Rights .............................................................. 40  
1. Chapter Overview ................................................................................................................... 40  
2. A Brief Review of Legal Adaptations to the Internet ............................................................ 40  
   a. Property and Trespass ....................................................................................................... 40  
   b. Cybercrime ....................................................................................................................... 46  
   c. Cyberwarfare .................................................................................................................... 50  
   d. Contract and Commerce ................................................................................................. 52  
   e. Copyright ......................................................................................................................... 53  
   f. Privacy ............................................................................................................................. 57  
   g. Defamation and Freedom of Expression ......................................................................... 62  
   h. Electronic Communications Spam .................................................................................. 65  
3. Finding a Common Theme ....................................................................................................... 68  
4. Digital Interests and Internet Rights ..................................................................................... 75  
   a. Anonymity, Privacy and Identity ...................................................................................... 75  
   b. Defamation, Copyright and Freedom of Expression ........................................................ 89  
   c. Email Spam ...................................................................................................................... 97  

Chapter 3 Personhood as a Substantive Theory of Legal Adaptation to the Internet ........... 104  
1. Chapter Overview .................................................................................................................. 104  
2. A Conception of Personhood ............................................................................................... 105  
3. The Internet for Personhood ............................................................................................... 114  
4. Implications of Personhood on the Internet ....................................................................... 122
a. Anonymity Protections ........................................................................................................ 122
b. Virtual Property ................................................................................................................ 125
c. Anonymous Defamation .................................................................................................... 131
d. Net Neutrality and the Internet as a Human Right ......................................................... 134

Conclusion .................................................................................................................................. 138

Bibliography ............................................................................................................................... 143
Introduction

It is trite to say that technological change often poses challenges to existing law in ways that necessitate legal adaptation. New technologies might, for example, alter the balance between economic social winners and losers,¹ or change the facts that either justify legal rules or to which legal rules apply.² They may also, as this thesis will suggest, expand existing interests or create entirely new interests along with corresponding methods of creating benefits or inflicting harms. If we believe that the law should reflect and protect the interests of those to whom it applies to any extent, then as technology changes, as with other forms of societal change, the law must change with it.

How the law should change in response to technological change is a more difficult question. At the dawn of a new technology, it can be impossible to know either how the technology will affect society or what the impacts of an early legal intervention might be.³ Respond too soon, and the response may be poorly tailored and have a worse impact upon society than the challenges raised by the technology. Respond too late, and the feared impacts of the technology may already have come to pass. There is also near unlimited breadth in the choice of both the process by which the law should respond and the substantive nature of its response. Given both the great uncertainty and the breadth of possible responses, the potential guidance offered by a theory of legal adaptation to technological change is highly valuable.

Unfortunately, theories of this type remain underdeveloped and there is only a limited universe of scholarship considering the issue of legal responses to technological change at all.⁴ There is, of course, a wealth of literature on the interaction between specific technologies and specific

¹ See Monroe E Price, “The Newness of New Technology” (2001) 22 Cardozo L Rev 1885 (noting that access to information brought about by technological change can change the balance of power between individuals and organizations at 1912)
³ The ongoing debates surrounding the proper balancing of copyright law can show just how uncertain the effects of legal policy might be, even where there are centuries of legal history to draw upon. See e.g. Michael A Carrier, “Copyright and Innovation: The Untold Story” (2012) Wis L Rev 891 (arguing that modern copyright law can impede innovation rather than promote it).
⁴ See Chapter 1, infra.
legal doctrines. But technological change, or even specific technologies, are rarely examined in a holistic manner. Instead, legal challenges raised by new technologies tend to be particularized to their doctrinal pigeonholes. Thus, for example, legal responses to the Internet are considered on the basis of copyright and the Internet,5 privacy and the Internet,6 warfare and the Internet,7 and so on. These assessments are undoubtedly useful assisting decision-makers on how to address particular problems and questions. However, in their narrow focus, they may fail to grasp the underlying interaction between individuals and the technology that gives rise to the need for legal adaptation in the first place. In order to better understand the relationship between individuals, society, and specific technologies, and to determine the underlying interests affected by specific technologies, a few scholars have called for a holistic approach that analyzes technologies across doctrinal boundaries.8 As it stands, such theories are rare.9

My goal in this thesis is to demonstrate that the development of such holistic and substantive theories of legal response to technological change are valuable and useful in guiding legal adaptation. In order to do so, I must meet three primary objectives. The first objective is to develop an approach to the creation of a substantive theory of legal adaptation to a given technological change. The second objective is to follow that approach in order to develop a substantive theory of legal adaptation to that particular technological change. The third objective is to demonstrate that such a completed theory is useful insofar as it can be applied to potential future challenges to the law created by that technology.

The Internet is a technology both substantially suited to, and in need of, a substantive theory of legal adaptation. It has been around long enough for there to be a significant amount of information concerning its impact upon society,10 but the challenges it raises for the law have not

---

5 See e.g. Jessica A Litman, “Copyright Legislation and Technological Change” (1989) 68 Or L Rev 275 (reviewing problematic attempts in the US to update copyright law to address new technologies, including computer programs at 334-336).
6 See e.g. Robert D Richards, “Compulsory Process in Cyberspace: Rethinking Privacy in the Social Networking Age” (2013) 36 Harv JL & Pub Pol’y 519 (examining the ability of existing law to address social media privacy).
9 I note Professor Bernstein’s work on genetic testing and the Internet as one exception: Bernstein, ibid.
10 Though it existed in research and military institutions long before, the Internet as we know it was made publicly available on August 7, 1991, giving it, for our purposes, an age of about twenty-four years. Old, perhaps, by
yet been resolved. Additionally, the development of the Internet and digital technologies has proved to be one of the most important challenges to many disparate fields of law,\(^{11}\) and there remain a large number of challenges still to be addressed. These include, for example, issues of attribution and proportionality in cyberwarfare,\(^ {12}\) questions of net neutrality and regulation,\(^ {13}\) protections for online anonymity and privacy,\(^ {14}\) and rights to virtual property.\(^ {15}\) Yet despite the academic attention given to online issues within specific areas of law, no comprehensive theory of legal adaptation to the Internet has yet been offered.

This is especially unfortunate given the massive impact the Internet has had the lives of individuals and on society. The effect of the Internet is more than that the sum of discrete identifiable legal issues. As United States Court of Appeals for the District of Columbia Circuit stated in a recent decision, the Internet “has transformed nearly every aspect of our lives, from profound actions like choosing a leader, building a career, and falling in love to more quotidian ones like hailing a cab and watching a movie.”\(^ {16}\) The Internet has thus become a part of our lives, and inextricable from modern society. Indeed, it has been said that the Internet is definitive of the modern era, which can therefore be called the “Information Age.”\(^ {17}\)

The extent of the profound differences created by the new networked society over those social forms of the past are not easily circumscribed in a single theory, and I do not attempt to do so

---

1. For a more complete review of the challenges raised by the Internet, see Chapter 2, Part 2, infra.
2. Concerns over attribution and proportionality with respect to the Internet stem from the question of how a victim state might attribute the attack to another nation if non-state actors are the perpetrators, and what a proportional response might be. See generally Dever & Dever, supra note 7 (discussing these issues in greater depth); Benjamin Mueller, “Why We Need a Cyberwar Treaty,” The Guardian (2 June 2014), online: <http://www.theguardian.com/commentisfree/2014/jun/02/we-need-cyberwar-treaty>.
here. This thesis instead illuminates only a few of the core interests expanded by the Internet, and the new mechanisms through which those interests can be harmed.

My thesis proceeds across largely unexplored territory, and much of the groundwork must be laid in the development of any theory. The first question is that of methodology. This thesis takes as its method a review and synthesis of existing legal adaptations to the Internet. Here, my focus rests firmly upon the laws of Canada and the United States. The purpose of this analysis is to find a common theme that might elucidate underlying concerns and interests that are giving rise to these legal adaptations, whether or not the decision-makers were aware of them.

The observed theme is that a number of the legal adaptations to the Internet disclose a recognition and respect for the manner in which the Internet expands deeply held personal interests. Despite some movements to the contrary, the law has, in many cases, given increasing protections to interests such as privacy, anonymity, freedom of expression, and freedom from intrusions into one’s personal space in the Internet context. While these are all premised upon existing rights, the additional protection of these interests online—sometimes in ways that appear to go beyond similar protections in the physical world—suggests that something fundamentally important to individuals is affected by the Internet. Indeed, in my view, these interests are made more important on the Internet because of the way the Internet expands the ability of its users to self-define, create meaning, explore the self, form identities, and ultimately pursue one’s goals. The Internet is thus an engine of personal growth and human flourishing that the law has sought to recognize. In doing so, the law has created a category of what I call “digital rights”: those rights that receive extra protection or special status in the Internet context.

Ultimately, these interests are personhood interests, as they are fundamental to that quality that makes us persons. I ground this notion of personhood in existential thought because it provides not only a foundational account of what it means to be a person, but also because it strongly accords with the import placed by the courts upon self-development and personal growth in protecting these rights. This view tells us that personhood is the freedom of persons to create meaning, continuously define themselves, choose their purposes, and seek those purposes. The Internet, it appears, allows us to do just that. The value of this theory lies in its applicability to

---

18 For a detailed discussion of these interests, see generally Chapter 2, Part 4, infra.
19 See Chapter 3, Part 2, infra.
future questions of how the law should adapt to technological change, and thus I conclude this thesis by looking at a number of such questions, including protections for anonymity on the Internet, recognition of virtual property rights, recourse for the defamation of pseudonymous identities, and the tangentially related issues of Internet access as a human right and net neutrality.

Chapter 1 of this thesis reviews the existing literature on legal adaptation to technological change generally, and observes that there are two primary types of theories on that issue: procedural and substantive. It lays some of the groundwork for such theories, including by categorizing the ways in which the law can invite legal adaptation. It justifies the importance of substantive theories of legal adaptation to technological change, as well as the importance of such a theory with respect to the Internet. It then establishes and justifies the methodology taken in this thesis of looking to existing examples of legal adaptation to the Internet in order to find a common theme, while noting some of this methods limitations.

Chapter 2 then proceeds to follow the method established in Chapter 1, briefly reviewing a broad swath of past legal adaptations to the Internet and the challenges raised by the Internet. A synthesizing analysis then consumes the remainder of the Chapter, which looks at the specific issues of anonymity protections, freedom of expression versus copyright and defamation, and new regulations concerning email spam. The chapter discusses the underlying rationales for each of these “digital rights” in depth, arriving at a conclusion that each demonstrates a regard for the personhood implications of the Internet, including its ability to function as a platform for learning and self-expression, its capacity to allow individuals to self-define and discover through the formation and assumption of identities and roles, and its capacity to allow one to write one’s own life narrative outside of local social norms that may be oppressive or coercive.

Chapter 3 takes on the problem of defining “personhood.” It does so by reference to existentialist thought, which views the person as an entity that must create meaning and constantly self-define in the face of the inherent pointlessness and absurdity of the universe. Through this lens, a person can be defined as an entity which is capable of defining itself and writing its own narrative, and personhood is the condition of being both free and able to do so. This conception takes existentialist thought only so far, and conceives as personhood ultimately as a form of freedom to self-determine. This view is similar to, but broader than, some common notions of autonomy in
that it holds that changes in the objective world, including technological change, can be expansive of personhood. This Chapter then argues that the Internet has been widely expansive of personhood, which underscores the creation of the aforementioned “digital rights.” The Internet thus gives rise to “Internet personhood,” which refers to the ways in which our use of the Internet becomes part of one’s self-definition. Finally, the chapter then turns to the application of this theory of Internet personhood to some potential future challenges posed by the Internet to the law such as the general regulation of rights on the Internet, virtual property rights, defamation of pseudonymous identities, and the issues of Internet access as a human right and net neutrality.

I conclude by providing a review of the findings of this study, addressing some of its limitations, and noting the many areas of potential future research.
1. Chapter Overview

There is limited scholarship on law and technological change, and while theories of legal adaptation to new technologies are frequently called for in the academic literature, they remain widely underdeveloped with respect to most new technologies. In Section 1 of this Chapter, I discuss what legal adaptation to technological change is and the kinds of challenges technology creates for the law. I then discuss why theories of law and technological change are important and what a theory of legal adaptation to technology should set out to do. In Section 2, I turn my attention specifically to the Internet to discuss its relevance and why a theory of legal adaptation to the Internet is important. Finally, in Section 3, I outline my approach to the development of a theory of legal adaptation to the challenges posed by the Internet and consider some limitations and possible objections to this approach.

2. A Theory of Legal Adaptation to Technological Change

a. What is Legal Adaptation to Technological Change?

There’s nothing new in the observation that new technologies can require legal adaptation, from modifications or deletions of existing rules, all the way to the formation of entirely new bodies of law.\(^{20}\) History is rife with examples of this sort of adaptation. For example, maritime law arises only because of the existence of the ancient technology of boats, and copyright law is largely a response to the fifteenth century technology of the printing press.\(^{21}\)

---

\(^{20}\) For example, as early as 1931, William Beard noted that “It may well happen that, as technology operates over ever larger areas, carrying standards and uniformity with it, we shall have to revise our whole concept of jurisdictions and local laws.” William Beard, “Technology and Political Boundaries,” (1931) 25 American Political Science Rev 557 at 571.

As technology is integral to our lives, it’s no surprise that the law would, in certain circumstances, need to change in response to technological progress. The daily experience of a modern person is vastly different from that of a person living five hundred or a thousand years ago. Technology has come to affect every area of human existence, from our food supply to how we communicate to how we maintain our health. Technology is a part of the fabric of society, and if the law is to be relevant to modern society, it must endeavour to keep pace.

Unfortunately, the academic consensus appears to be that the law lags behind technological change. Nonetheless, over the past few decades, numerous new technologies have challenged existing legal regimes or demanded the development of new law, and have therefore led to legal adaptation. Some examples include technologies related to *in vitro* fertilization, weather modification, human cloning, and genetically modified organisms. The Internet has also proved to be challenging to existing legal regimes across a number of doctrinal categories. And the law will likely be challenged in the future by technologies such as nanotechnology, cryogenics, and artificial intelligence. Each of these technologies is unique in the way it affects individuals and society, and therefore each requires the law to address it individually, if legal adaptation is warranted at all.

The question of when legal adaptation is warranted is a difficult one, and it’s one with which courts, legislators and administrative bodies must struggle every time a new challenge is raised by a technology. Technology can bring about a need for doctrinal adaptation in a number of different ways. Indeed, recognizing the many ways in which technology can challenge the law is

22 See e.g. Lyria Bennett Moses, “Agents of Change: How the Law ‘Copes’ with Technological Change” (2011) 20 Griffith L Rev 763 (reviewing other commentators on the law’s failure to keep pace with technology at 763-764) [Moses, “Agents of Change”]; Bernstein, supra note 8 at 967.
26 Ibid at 78-79.
27 See e.g. Litman, supra note 5 at 334-336 (with respect to copyright law); Richards, supra note 6 (examining the ability of existing law to address social media privacy); Dever & Dever, supra note 7 (showing the uncertainty of applying the traditional law of war to cyberwarfare); Steven Kam, “Intel Corp. v. Hamidi: Trespass to Chattels and a Doctrine of Cyber-Nuisance” (2004) 19:1 BTLJ 427 (discussing the tort of trespass to chattels and nuisance in the online space); Robert A Hillman & Jeffrey J Rachlinski, “Standard-Form Contracting in the Electronic Age” (2002) 77:2 NYUL Rev 429 (discussing the new dimensions of standard form contracting on the Internet).
28 See generally Friedman, supra note 2.
the first step in understanding the relationship between the law and technology, and it lays the groundwork for any theory of legal adaptation to technology. Because of this, as some scholars have recognized, a classification scheme of the ways in which new technologies invite legal adaptation is helpful at the outset to provide context to the ensuing discussion of theories of legal adaptation to technological change.

Professor David Friedman has argued that technological change can affect the law in at least three ways:

(1) by altering the cost of violating and enforcing existing legal rules; (2) by altering the underlying facts that justify legal rules; and (3) by changing the underlying facts implicitly assumed by the law, making existing legal concepts and categories obsolete.\(^{29}\)

However, this taxonomy is problematic in that it appears to only address technologies that affect existing legal rules, rather than those technologies that might, absent new law, be effectively unregulated.\(^{30}\) For example, weather modification techniques, when first developed in the 1940s went largely unregulated throughout much of the 1950s, leading to numerous independent businesses that, for a fee, would attempt to seed cloud formation over agricultural regions.\(^{31}\)

While it could be argued that this technology altered “the underlying facts that justify legal rules,”\(^{32}\) given that there were at the time no legal rules directly concerning weather modification to justify, it does not seem to fit. Additionally, all three of these categories strongly overlap. Indeed, it would be easy to read categories (1) and (3) as species of category (2). After all, the cost of violating and enforcing legal rules are also the facts by which legal rules are justified, as are those facts implicitly assumed by the law.

Professor Lyria Bennett Moses has also proposed a categorization scheme that looks specifically at the ways in which the law might respond to technological change. Her scheme is as follows:

1. **New rules.** We need to regulate certain new forms of conduct and new, specially tailored laws are required to do this. In some cases, it may even be

---

\(^{29}\) *Ibid* at 71.

\(^{30}\) By unregulated, I mean in the sense that no legal rules specifically contemplate the activity or conduct in question. It remains possible, and likely, that laws of general application will apply, but here I refer to those situations where the law is largely permissive of the conduct by virtue of the lack of conduct-specific regulation.

\(^{31}\) Harris, *supra* note 24 at 29.

\(^{32}\) Friedman, *supra* note 2 at 71.
appropriate to ban a particular technology or particular applications of that technology.

2. **Uncertainty.** The law is uncertain as it applies to new forms of conduct. In other words, it is not clear whether such conduct is commanded, prohibited, or authorized. Existing rules need to be clarified.

3. **Scope of rules.** Existing rules were not formulated with new technologies in mind. Thus, some rules in their current form inappropriately include or exclude new forms of conduct.

4. **Justification for rules.** Some existing rules are explicitly or implicitly based on a premise that no longer exists, and are thus no longer justified [or important or cost-effective].

This categorization is more complete and more useful, but it’s also unfortunately overly simplistic and, in some cases, confusing.

The first of Moses’ categories, new rules, is overly broad. It fails to differentiate among the many different kinds of challenges that new technologies can create that might require new rules. Instead, like most of these categories, it focuses on how the law might need to respond, rather than what sorts of challenges the law might be required to address through adaptation. Whether a technology requires new rules is a normative question that must be determined after finding that a new technology creates a challenge for the law. New rules may be necessary to address a wide variety of functionally different concerns. The same is true of Professor Moses’ third category, which refers to modifications to the scope of rules. The law might need to determine whether or not a new technology should fall under an existing rule for a wide variety of reasons, and again, this tells us little about the nature of the underlying challenge to the law.

These categories are also incomplete. For example, as will be discussed below, they neglect to address technological change that alters the meaning or application of existing rules.

As the above analysis indicates, it’s important to conceptually separate the categories of how the law might respond to new technologies from the categories of challenges to the law created by

---

new technologies. I set out to examine the latter first. In my view, the types of challenges to the law created by technological changes can be reduced to five categories.

The first category of technological challenges for the law is that of technologies that have externalities, whether negative or positive, when used by individual actors. Examples of technologies with negative externalities would include weather modification technologies and technologies that create pollution or environmental impacts. Regulation is often necessary to ensure that the negative external effects are limited and that the actor responsible for negatively affecting others absorbs the costs of the harms, or takes steps to minimize or eliminate the harm to others. Technologies with positive externalities, on the other hand, may invite legal adaptation to ensure their adoption. These technologies invite legislative or administrative embrace in order to improve efficiency or general well-being by virtue of their externalities. These technologies tend to be technologies of general societal benefit, but which may not be generally adoptable by individuals, where individual adoption is slow, or where necessary legal infrastructure is not in place to support their use. An example of a legal response to these technologies would be government incentives to purchase electric vehicles, such as that offered by the Government of Ontario.34 It may also include, for example limitations on the use, manufacture or trade of older technologies to promote newer ones, such as restrictions on incandescent lightbulbs in Canada.35

The second category consists of technologies that require coordination and central control to properly function, such as for aviation, general automobile traffic, telecommunications systems, or the electric power grid. Without coordinating laws these technologically-based systems would fail to operate, would be highly inefficient, or would become extremely dangerous.

The third category is that of technologies that create new harms or dangers, increase the risk of harm, or create new methods of inflicting harm. This is a broad category of technologies that includes, for example, the new physical dangers posed by automobiles or airplanes, the possible harms of genetic engineering, or the risks of privacy invasion on the Internet. I note that there is

35 While not expressly restricted, Canada’s Energy Efficiency Act and the Energy Efficiency Regulations effectively prevent the interprovincial trade of incandescent household lightbulbs by requiring all household lightbulbs to meet efficiency standards that incandescent bulbs cannot meet. See Energy Efficiency Act, SC 1992, c 36 s4(1); Energy Efficiency Regulations, SOR/94-651, Schedule I, items 136-136.3.
some overlap here with the first category, in that both necessarily involve the creation of harms or risk of harm. However, I separate them on the basis that the first category contemplates those technologies that have inherent externalities to their use, whereas this category contemplates technologies that do not necessarily have externalities when used, but which raise the possibility of either being used to inflict direct harm, or which might create the risk of direct harm. As will be discussed further in Chapter 2, a new technology may raise the prior question of whether a claimed harm is a harm at all.

The fourth category—which combines all three of Professor Friedman’s categories—is that of technologies that alter the facts justifying existing law. This may render a given law obsolete, may require the alteration of a law, or it may require entirely new rules. Again, we must be cognizant not to confuse how the law should respond to a technological challenge with the types of challenges posed by new technologies. Examples within this category are many. It includes cases where technological advancement has rendered certain laws obsolete. Professor Moses notes that, for example, the emergence of railways rendered some rules pertaining to easements obsolete. Another example she provides is that of legal regulation designed to prevent interference in the use of radio spectrum, many of which became unnecessary with advancements in radio technology. This category also includes cases where the balance of a legal regime has been changed by altering the costs and benefits of the conduct to which it pertains. For example, both photocopiers and copyright altered the legislative balance between users of works and copyright owners, leading to changes in regulation.

This category also includes technologies that redistribute wealth or power or alter the balance of winners and losers in society. The development of copyright law in response to the printing press is one example, in that the printing press gave great power to the printers and booksellers, while reducing the wealth of scriveners and book binders, while still giving little to authors. Technologies that eliminate jobs, transfer wealth, or empower certain groups of people will

36 Specifically, Moses refers to the rule that an easement was only proprietary rather than personal where the person to whom the easement applied owned adjoining property. Where railways were the subject of the easement, this no longer made sense. Moses, “Why Have a Theory”, supra note 33 at 590-591.
37 Lyria Bennett Moses, “Recurring Dilemmas”, supra note 33 at 267-268.
38 See generally Litman, supra note 5.
39 See e.g. Price, supra note 1 (noting that access to information brought about by technological change can change the balance of power between individuals and organizations at 1912).
40 See generally, Morris, Jr, supra note 21.
typically fall within this category. Technologies such as human genetic engineering or medical technologies that extend the life of those able to afford it raise similar distributional issues that a legislature may wish to address.

A special case of this fourth category is technological change that alters the meaning or enforcement of a law. Examples of this category are often technologies that allow for more accurate measurement or more complete detection of regulated activities. Professor Max Stul Oppenheimer has addressed this issue at length, and he provides the example of legislation that requires ‘zero emissions’ of certain pollutants. He notes that, in such statutes, the word ‘zero’ really means ‘below detectable limits’. Thus, as detection technology improves, a law that requires zero emissions effectively changes to demand fewer actual emissions. If existing legislation was crafted to reflect the ability of current technology to measure a factor, such as levels of a pollutant, it may not be properly tailored when newer technology refines that measurement. Similarly, technology may increase the ability of authorities to enforce various rules. The development of the breathalyzer, for example, provided an increased ability to measure blood alcohol level, and therefore to police impaired driving. Such technological advancements may lead to a change in legal definitions or standards, as it did in the creation of the Canadian maximum blood alcohol standard for operating a motor vehicle of “eighty milligrams of alcohol in one hundred millilitres of blood”.

The fifth category is technology that changes the scope of existing law. In this category are those new technologies that may be governed by existing laws and, by virtue of their potential inclusion under existing law, might effectively increase the scope of the regulated conduct. The challenge will typically relate to whether it’s appropriate for the existing law to govern the new technology. For example, in Brookfield Communications, Inc. v. West Coast Entertainment Corp., the United States Court of Appeals for the Ninth Circuit was faced with the issue of

---

42 Ibid at 5.  
43 Oppenheimer gives the example of speed limits. He argues that if a legislature determines that cars should not be able to go above 75mph on a given road, and if speedometer measurement technology only has a precision of 5mph, then a speed limit might be set at 70mph so that the determined actual maximum of 75mph is still allowable within the standards of measurement. However, if speedometers improve to allow precision within 1mph, then the effective maximum speed becomes 71mph, which may be less efficient than originally intended. Ibid at 6-7.  
44 Criminal Code, RSC 1985, c C-46, s 253(1)(b).
whether trademark and unfair competition law extended to Internet domain name registrations. Issues in which the application of an existing law to a new technology are uncertain will generally fall within this category. This differs from the fourth category (changing the facts justifying existing rules) in that the justification for the existing rules doesn’t change with respect to their original purpose, but rather that justification might simply be inappropriate for the new technology.

There is clearly some overlap in these categories, and a given technology may raise legal challenges in multiple ways and implicate multiple categories. For example, commercial aviation raises challenges for the law in ways described by, at a minimum, the first three categories. The first category applies because commercial aviation has negative externalities such as noise pollution that may be regulated. The second category applies because commercial aviation requires coordinating legislation to function properly. The third category applies because air transportation raises a number of safety concerns and exposes both passengers and bystanders to dangers. Commercial aviation may involve the other categories as well, though an analysis of such is outside the scope of this chapter.

b. When is Legal Adaptation Necessary?

Given the many ways in which new technologies can raise challenges for the law or invite legal adaptation, does all technological change require legal adaptation? The answer to this is, of course, no. It’s likely that only a small percentage of new technologies require new law. In most cases, existing law will be sufficient to cover technological advances, and no legal change will be warranted. For example, the theft of a digital watch is no different from the perspective of the criminal law than the theft of an analogue one. Or consider the difference between a manual razor and an electric one. It seems unlikely that the electric razor requires any new legislation over and above any that might apply to the manual razor.

---

45 The Court found that it did. *Brookfield Communications, Inc v West Coast Entertainment Corp*, 174F (3d) 1036 (9th Cir 1999).
46 *Canadian Aviation Regulations*, SOR/96-433, s 507.20.
47 See e.g. *Aeronautics Act*, RSC 1985, c A-2.
48 See generally *ibid*. 
However, there is some need for caution in making such statements. Individual technologies do not merely affect a single area of law. Indeed, a given technology will almost always intersect with numerous doctrinal categories, each of which may treat the new technology in a manner similar to, or different from, older technologies. Indeed, a new technology is likely to be governed by a large number of existing doctrines that need not treat the new technology in a different manner from older technologies, but in some cases, one or more of these doctrines will differentiate between the old and new technologies. For example, as mentioned above, we might not expect an electric razor to raise many new legal concerns. A theft of an electric razor is the same from the perspective of the criminal law as the theft of a manual razor. Its sale is unlikely to raise any new issues from the perspective of consumer protection regulations or sale of goods regulations, and we can expect tax treatment of the sale to remain the same when compared to the manual razor. However, it will likely be treated differently from a manual razor from the perspective of environmental stewardship laws that relate to the recycling of electronic goods.\footnote{For example, Ontario’s \textit{Waste Electrical and Electronic Equipment} regulation expressly prescribes electric razors as subject to electronics stewardship requirements. \textit{Waste Electrical and Electronic Equipment}, O Reg 393/04, Schedule 1, item 34.} Thus, a new technology may raise legal challenges that are only relevant to specific doctrinal categories, or in ways that require only very limited adaptation.

We must also be careful not to suggest that all potential challenges to the law raised by new technologies ultimately require legal adaptation. Often, these challenges can be answered by existing law merely by clarifying the application of existing doctrines to new technologies. While the clarification that existing law applies to a new technology can be seen as a form of legal adaptation to that new technology itself, it is a much more limited form of adaptation insofar as it effectively alters the scope of the law rather than its content. It’s also more limited because the choice before the decision-maker was a binary one, rather than open-ended choice of regulation. Indeed, a clarification that existing law applies can often be seen as a preliminary (and occasionally erroneous) finding that legal adaptation is not necessary.

Where clarification is necessary, the issue typically comes before the courts to determine whether a certain new technology fits within an existing legal regime. Examples of these types of
issues include whether an automobile is sufficiently like a carriage to allow a doctor in debt to keep it for his business,\(^5\), or whether a hyperlink to defamatory content constitutes publication.\(^5\)

In the former case from 1916, a debtor physician attempted to retain his automobile under a statute that allowed debtors to retain a “horse and vehicle” when necessary for their occupation.\(^5\) The court determined that since the purpose of the exemption was to allow a debtor to keep a vehicle so that he might continue to work, it makes sense to read an automobile into the statute.\(^5\) This finding is readily understandable. An automobile may be a technological advancement upon the older technology of a horse and cart contemplated by the statute, and it may have numerous advantages, but so far as the law pertaining to debtors was concerned, these were easily analogized for the purpose of the statute. The court effectively found that legal adaptation, here, was unnecessary.

As stated, from some perspectives, the mere application of existing law to a new technology might be seen as a form of legal adaptation. After all, some might view a decision that an existing legal regime applies to a new circumstance as a landmark decision that will change the behaviour of numerous actors. Regardless, in my view, this is a much more limited form of adaptation, if it can be called adaptation at all, that doesn’t truly change the content of the law, but rather its scope.

Similarly, in the much more recent case of *Crookes v Newton*, the Supreme Court of Canada was faced with the issue of whether hyperlinking to defamatory content constituted publication of that content, and would thus make the poster of the hyperlink liable for defamation. The Supreme Court held that it did not. As the Supreme Court of Canada reasoned, while a hyperlink may allow faster access to a defamatory publication than a written reference, both ultimately perform the same function.\(^5\) Both merely point to a source, and both require positive action on the part of the reader. Once again, the reasoning is quite clear. The Supreme Court determined

---

\(^5\) *Prater v Reichman*, 135 Tenn 485 (Tenn Sup Ct 1916).


\(^5\) Keith A Christiansen, “Technological Change and Statutory Interpretation” (1968) 49:2 Wis L Rev 556 (discussing the statute construed in *Prater v Reichman*, supra note 30, at 563).

\(^5\) Ibid.

\(^5\) *Crookes v Newton*, supra note 51 at paras 22-27.
that the new technology fit neatly into existing law by way of analogy. If a reference to a defamatory source is not itself defamatory, neither should be a hyperlink.

In a sense, in both of these cases, the courts determined that the technological change was a change in degree, rather than a change in kind, from the technologies and conduct already contemplated by the law. The hyperlink was a change in degree from that of a textual reference, insofar as it simply made accessing the referenced work more convenient and direct for the user. It was still fundamentally a reference. The automobile, likewise, was only a change in degree from that of a horse and carriage for the purposes of a physician being able to make house calls and travel as part of his occupation. While it may be faster and require less maintenance, it is merely another mode of transport relied upon for the purposes of the debtor’s medical practices. The law will only need to truly adapt through changes to the content of the law where, for the purposes of a given legal regime, a new technology appears to create a change in kind, or at least a change in degree great enough to upset the assumptions of the law.

Unfortunately, there can be no bright line test for determining whether a technological change requires legal adaptation. Instead, as this thesis argues, this must be carried out on a context-specific basis by understanding the challenges posed to the law by the new technology, and then determining whether those challenges are significant enough to warrant a response.

c. How Can the Law Respond to Technological Change?

Where a new technology does raise legal challenges, and cannot easily be clarified as falling into a traditional category, the next question that must be asked is how can the law respond? Here we are concerned with generally defining the means through which the law can adapt, regardless of the legal institutions responsible, which are briefly discussed in Part II. In my view, there are four primary legal responses that can be made, which largely correspond to Professor Moses’ categorization of legal challenges, discussed above.55

Firstly, and most obviously, new law or regulations can be created that contemplate the new technology and its corresponding conduct or impact. These might take the form of comprehensive statutory or regulatory schemes targeted at a single technology, such as Canada’s

55 See Moses, “Why Have a Theory”, supra note 33 and accompanying text.
Aeronautics Act\textsuperscript{56} and Air Transportation Regulations\textsuperscript{57} for airplanes. It might also take the form of multiple technology-specific rules being included in various areas of law. For example, legal responses to the Internet in Canada have included, among other things, specific rules pertaining to consumer contracts made over the Internet,\textsuperscript{58} to criminal sanction for hacking a computer system,\textsuperscript{59} to prohibitions on sending unsolicited commercial email messages.\textsuperscript{60} In either case, they result in the creation of rules that are fundamentally new and technology-specific. New agencies or firms may also be created or empowered to adjudicate new issues and create new rules, as with the empowerment of non-profit ICANN by the US government to govern domain name disputes on the Internet.\textsuperscript{61}

Secondly, existing legal regimes can be modified to better address the new technology, which can encompass repealing outdated laws, or modifying existing ones. For example, copyright law in Canada is interpreted as being largely technologically neutral,\textsuperscript{62} but the balance struck between copyright owners and the users of works is updated to reflect the impact of new technologies.\textsuperscript{63} Naturally, there is conceptual overlap between creating new rules and modifying existing rules, and the two cannot always be differentiated. For example, it may not be clear whether the creation of Ontario regulations pertaining to consumer “Internet Agreements”\textsuperscript{64} are new rules, the modification of existing consumer protection legislation, or a clarification of how existing rules apply. Despite this conceptual overlap, the different categorization is useful for the many cases in which it’s clear whether there has been a modification of a rule (such as where a statutory rule has actually been changed in response to a technology) and where wholly new

\textsuperscript{56} Aeronautics Act, supra note 47.
\textsuperscript{57} Air Transportation Regulations, SOR/88-58.
\textsuperscript{58} For example, the Ontario Consumer Protection Act has special regulations for “Internet Agreements.” Consumer Protection Act, 2002, SO 2002, c 30, Sch A, ss 37-40.
\textsuperscript{59} Criminal Code, supra note 44, s 342.1(1)(a).
\textsuperscript{60} See generally An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, SC 2010, c 23 [CASL].
\textsuperscript{61} ICANN is an acronym for the Internet Corporation for Assigned Names and Numbers. For a more detailed explanation of the origins of ICANN, see David G Post, In Search of Jefferson’s Moose: Notes on the State of Cyberspace (Oxford: Oxford University Press, 2009) at 148-158.
\textsuperscript{63} The Preamble to the Copyright Modernization Act of 2012 makes it clear that many of the changes are a response to the Internet: “advancements in and convergence of the information and communications technologies that link communities around the world present opportunities and challenges that are global in scope for the creation and use of copyright works or other subject-matter”. Copyright Modernization Act, SC 2012, c 20, Preamble.
\textsuperscript{64} Consumer Protection Act, supra note 58, ss 37-40.
rules have been created (such as where comprehensive technology-specific statutes are introduced). Organizational changes, such as moving administrative or decision-making power to new agencies or organizations will also generally fall within this category.

Lastly, the law can either do nothing, or expressly include a new technology under an existing doctrinal category. As I’ve argued, expanding the scope of an existing rule solely to encompass a new technology is a limited form of legal adaptation, but it is an option available when new technologies raise challenges for the law. The Canadian Revenue Agency’s classification of Bitcoin as a commodity for tax purposes rather than a currency\textsuperscript{65} that might require new rules is one example of addressing a challenge by placing it, rightly or wrongly, into an existing legal category. The desire to wait and see, or to use existing rules provisionally until a need for legal adaptation is clearly demonstrated, is understandable. There is obvious merit to delaying a legal response until sufficient information is gained to understand how best to respond.\textsuperscript{66} Time is needed to consider the impacts of technology, and legislation too soon may lead to undesirable and poorly-tailored laws.\textsuperscript{67} The time may be taken to consider how best to procedurally adapt the law, such as through the courts, administrative agencies, or legislation. Additionally, in some cases, self-regulation may be promoted in certain technologically-based industries, as happened in the case of online behavioural advertising, which is currently self-regulated in Canada.\textsuperscript{68}

The law can, of course, simultaneously respond in all three ways to the same technology across different doctrinal categories.

3. **Why Have a Theory of Legal Adaptation to Technological Change?**

As the above analysis makes clear, a need for a legal response to technology can occur in a variety of unique ways, and adaptation can also take a number of distinct forms. These


\textsuperscript{66} See Moses, “Agents of Change”, supra note 22 (discussing the dangers of rushing into new legislation in response to technological change at 765).


\textsuperscript{68} The Digital Advertising Alliance of Canada, which consists of numerous advertisers, currently self-regulates much of the online behavioural advertising occuring in Canada. See “About the DAAC,” online: Digital Advertising Alliance of Canada <http://youradchoices.ca/about-the-daac/>.
categorizations are useful in understanding the interaction between law and technology, but they’re only the first step to understanding when and how the law should adapt in response to any given technology. It’s in answering this normative question that theories of legal adaptation to technological change can assist.

Unfortunately, legislatures and courts are often hamstrung in their ability to respond to technological change by the inherent uncertainties that accompany technological development. It’s rare that one can predict with confidence, for example, how a new technology might influence the behaviour of individuals or how it might alter the balance of power between individuals and organizations.

The problem with responding to new technologies arises from the simple observation that in order to properly adapt the law to a new technology, we must first understand not only the immediate utility of that technology, but also its social, political and economic dimensions. This is a complex issue, as every technology is different, and any one of these dimensions can change over time. The legal and social relationship to technology is not a fixed value, but one dependant on countless other dynamic factors and conditions. Consider the role played by the automobile in human life. What started out as a simple convenience has, over time, become relevant to everything from urban planning to climate change to privacy law.

It’s in understanding how a new technology affects people, their activities and relationships, as well as how it affects the law, that theories of legal adaptation to technological change are

---

69 Moses, “Why Have a Theory”, supra note 33 (“Technological change is usually more difficult to foresee at the time a law is drafted” at 599).
70 The ongoing copyright debates concerning the economic effects of new technologies and any given legal change on copyright interests are a great exemplar of the uncertainty of technological and legal change upon affected parties: see e.g. Friedman, supra note 2 (reviewing responses in copyright law to new technologies at 73-75); Litman, supra note 5 (reviewing problematic attempts in the US to update copyright law to address new technologies, including computer programs at 334-336); Carrier, supra note 3 (arguing that modern copyright law can impede innovation rather than promote it).
71 See Cockfield, supra note 8 (discussing other areas of study that have addressed the dynamic relationship between technology and society at 401).
74 See e.g. R v Caslake, [1998] 1 SCR 51, 155 DLR (4th) 19 (concerning evidence taken from the search of a vehicle and the accused’s right to privacy).
relevant. Law tends to lag behind technological developments.\textsuperscript{75} This may lead to outdated laws that have little relevance to the issues facing members of a society, and which fail to address the true interests of those affected.\textsuperscript{76} It may also lead to harms without a remedy.\textsuperscript{77} When this happens, justice may be rendered incomplete or it might be undermined entirely. In other cases, special interests may push for remedies for perceived harms we may not want to provide. In any case, a theory of law and technological change can help the law keep up with technological change by identifying when change is needed, why, and how that change can be best implemented to solve the problem.\textsuperscript{78}

Theories of legal adaptation to technological change are, then, scholarly roadmaps that assist in figuring out where the law stands with respect to a new technology, what interests are affected by a new technology, whether to respond, and how best to respond or arrive at a resolution.

But what does a theory of legal adaptation to technological change look like, and what should it contain? A review of the scholarship demonstrates that theories of legal adaptation to technological change can be divided into two broad categories: procedural and substantive.

\textbf{a. Procedural Theories}

Procedural theories focus on the mechanisms through which legal adaptation can be achieved, rather than looking at what kinds of adaptations should be made to respond to a given challenge. They are, in other words, institutionally focused. These assist in deciding whether it’s preferable for regulations with respect to new technologies to be made, for example, iteratively through administrative agencies designed for the purpose, through judicial response, or whether the blunt instrument of legislative change is preferable.\textsuperscript{79}

Professor Lyria Bennett Moses has written extensively on this topic, especially with regard to Australia.\textsuperscript{80} She’s considered in detail the many actors that have been involved in adapting the

\textsuperscript{75} See e.g. Moses, “Agents of Change”, \textit{supra} note 22 (reviewing other commentators on the law’s failure to keep pace with technology at 763-764); Bernstein, \textit{supra} note 8 at 96.
\textsuperscript{76} \textit{Ibid}.
\textsuperscript{77} See e.g. \textit{Jones v Tsige}, 2012 ONCA 32, 108 OR (3d) 241 (in which the plaintiff would have been left without a remedy had the court not recognized the tort of intrusion upon seclusion).
\textsuperscript{78} See Bernstein, \textit{supra} note 8.
\textsuperscript{79} For more on procedural issues relating to legal adaptation to technologies, see generally Moses, “Understanding Legal Responses”, \textit{supra} note 23; Moses, “Agents of Change”, \textit{supra} note 22.
\textsuperscript{80} Moses, “Agents of Change”, \textit{supra} note 22.
law in response to technological change, including, as she says, “committees, government departments, royal commissions, law reform organisations, technology assessment agencies, ethics bodies, [and] courts,”\textsuperscript{81} among others. She concludes that legal responses are often done piecemeal, and that more should be done to coordinate the different responsible groups to ensure a more holistic response to a challenge raised by technological change.\textsuperscript{82} She has also considered the various strengths and weaknesses of courts and legislators at responding to legal change, finding each is better suited to certain kinds of change than others.\textsuperscript{83}

Procedural theories also address the general principles that should guide decision-makers when responding to technological change. Professor Arthur Cockfield has argued that legal responses to technological change can be divided up into two categories: liberal and conservative.\textsuperscript{84} In his conception, a “liberal” response merely means one less deferential to past legal doctrines and more open to addressing the interests affected by new technologies. By contrast, the conservative view relies more on past precedent and is less responsive to real interests.\textsuperscript{85} He prefers the liberal mode. In other words, where institutions are faced with challenges brought by new technology, Professor Cockfield argues, they should be more willing to consider the real-world effects of the technology rather than trying to shoehorn new technologies into old rules. While Cockfield’s categorizations suggest a preference for certain kinds of substantive legal responses to technological change, his categorization has an institutional focus and is more concerned with the involvement of existing doctrine, rather than determining the response itself. In a different paper, he and Jason Pridmore argue that, during periods of technological change, decision-makers should be more forward looking, and less reliant on existing doctrine,\textsuperscript{86} further demonstrating the institutional focus of his work.

In a similar vein, a paper by Monroe Price and John Duffy, might suggest that taking too “liberal” (to use Cockfield’s term) a view of legal responses to technological change, and thus to limit the importance placed on past doctrine, can give perhaps too much discretion to decision-

\textsuperscript{81} Ibid at 763.
\textsuperscript{82} Ibid at 785-786.
\textsuperscript{83} Moses, “Adapting the Law”, supra note 67.
\textsuperscript{84} Cockfield, supra note 8.
\textsuperscript{85} See generally ibid.
\textsuperscript{86} See generally, Cockfield & Pridmore, supra note 8.
makers to enact their own agendas. Price and Duffy specifically looked at American courts and legislators to argue that, despite frequently discussing major reform, the legislators actually tend to move more conservatively with respect to new technologies than the courts. Indeed, they accuse the courts of often using technological change as an excuse to further their policy goals, such as those with respect to the First Amendment right of freedom of speech. While this may be true, I suspect that it has little to do with technological change specifically, and that courts incentivized to alter the law towards their preference would use any kind of change, whether it arise from social or political change, or a new technology. In any event, Price & Duffy argue that technological change, even radical technological change, is not enough on its own to warrant changes to judicial doctrine. In a later paper Professor Price appears to have modified, or at least clarified, this argument somewhat, suggesting that technological change can have significant effects upon society that warrant change in certain circumstances, while maintaining that technological change is not, in itself, sufficient to warrant discussions of legal adaptation.

Another kind of procedural theory might look more broadly at how law should be fundamentally designed to keep pace with technological change. David Howes has written a fascinating article arguing that the form in which laws are communicated has an effect upon the design of their contents. He argues that, when the dominant form of communication transitioned from oral to textual, the law underwent a change from being more flexible, responsive and multicentric to being predominantly centralized, consistent, and authoritative. He argues that with the increasing use of the Internet for human communication and the promulgation and access to law, our laws may begin to become more flexible and multicentric than they are now. Specifically, they may reflect a notion of deliberative democracy, in which they are formed through online discussion and debate rather than existing legislative processes. Thus, when faced by a technological challenge, the law will respond by deliberative action based upon the consensus of the polity rather than traditional institutions. While little deliberative democratic reform appears to have occurred in the fifteen years since the publication of the article, the idea that legal adaptation to

88 Ibid.
89 Ibid at 1008.
90 Ibid at 1015.
91 See generally Price, supra note 1.
93 Ibid at paras 21-23.
technological change can be made through deliberative means may be relevant to procedural theories of legal adaptation to technological change. It also suggests that the procedure by which technological change is addressed could itself be affected by technological change.

Similarly, Professors Anthony Casey and Anthony Niblett have suggested that technological advances in the areas of artificial intelligence and data collection will fundamentally alter the manner in which laws are promulgated and structured.\(^94\) Specifically, they contend that computer systems with artificial intelligence will be able to provide individuals with micro-directions to guide their behaviour and activities. These micro-directions would take the form of a complex system of rules that would take into consideration the individual circumstances and come to a determination.\(^95\) While the authors’ views of the capabilities of artificial intelligence technologies, and their relative dismissal of the possibility of systemic error or bias, is perhaps overly optimistic, it nonetheless presents one possibility for how the law can both procedurally remain apace with technological change through the use of new technologies itself.

Further, procedural theories might also look at the impact of special interests and political influence upon law reform. Lobbyists, large corporate interests, and others with political or social power can often push for laws that may or may not be in the public interest. These entities may use the spectre of technological change to push for increased rights or protections for their own interests. For example, the United States Congress has been accused of giving large copyright-owning firms the ability to craft their own copyright legislation, especially in response to technological change.\(^96\) The reality of modern lawmaking is that it’s a complex political process, and there is certainly much that can be said about it with respect to technological change. However, such a discussion moves beyond even a discussion of law and technology as criticisms of government functions of this sort relate to all aspects of lawmaking, regardless of the involvement of technologies.

The forgoing discussion shows that procedural theories are broadly applicable to technological change, and largely look at how modern states can arrange their institutions and policies in order


\(^{95}\) Ibid.

\(^{96}\) Jessica Litman, “Real Copyright Reform” (2010) 96 Iowa L Rev 1 at 11.
to be responsive to technological change. These theories are generally uninterested in what it is about a given technology that gives rise to a problem for the law, leaving that analysis to be carried out by whatever institution or process is promoted as best being able or used to respond.

b. Substantive Theories

In contrast to procedural theories, substantive theories look at individual technologies and how the law responds to them. They aim to get at the root social causes of the challenges that are raised by a technology, rather than focus on the institutional mechanisms for how the law might adapt. They’re specific to technologies, but not specific to any one doctrinal category insofar as they attempt to look beneath doctrinal categorization to address the impacts of a technology more holistically.97 Most often, new technologies are only analyzed with respect to existing legal fields.98 Thus, responses to the Internet are divided up into the Internet and copyright law,99 the Internet and privacy law,100 the Internet and contracts,101 and so forth. There is nothing wrong with such analyses, and they uncontroversibly offer important perspectives and ideas about how to adapt the law. However, in their narrow focus they may miss unifying themes and issues that a more holistic approach may elucidate. This is the knowledge gap that substantive theories of legal adaptation to technological change seek to fill.

Calls for such substantive theories have been made in the academic literature. Professor Gaia Bernstein has written, with respect to legal responses to technology, that we need a “socially oriented approach that focuses on the impact of technological innovation on social structures, institutions, and values and on our ability to mold these social influences by restructuring uses of new technologies.”102 She argues that too much modern scholarly analysis remains limited to doctrinal pigeonholes and therefore fails to address the overarching changes created by innovation and technological change. She therefore calls for a more comprehensive approach to new technologies in order to address the root social concerns.103

97 Bernstein, supra note 8 at 697; Cockfield, supra note 8 at 387.
98 Ibid.
100 See e.g. Jacqueline D Lipton, “Mapping Online Privacy” (2010) 104 Nw UL Rev 477.
101 See e.g. Hillman & Rachlinski, supra note 27.
102 Bernstein, supra note 8 at 966.
103 See generally Ibid.
Professor Bernstein is not alone in making this call. Professor Cockfield has also promoted this kind of doctrinally-agnostic approach. He argues that a holistic approach to understanding the legal and social impacts of a technology

would act as one more tool within a scholar's methodological toolbox to promote more fully informed legal analysis. It should not seek to replace existing avenues of enquiry such as intellectual property law, but should co-exist along with other areas of technology law.¹⁰⁴

In his view, the purpose of a theory of legal adaptation to technological change is to assist in probing the real interests affected by technological change, and finding solutions where those interests need to be protected against the adverse impacts of a technology.¹⁰⁵ He does not seek to establish new areas of legal doctrine, or to create new fields of law, but to use the adaptations made within individual doctrinal categories to illuminate the impacts of the technology more broadly so that the new insights can be used within existing doctrinal categories. Indeed, in another article, Professor Cockfield and Jason Pridmore restated this argument in the following terms:

a law and technology theory could draw from these compartmentalized doctrinal boxes and reflect back on them with a broader perspective, so that legal analysis would be better informed by taking a fuller accounting of the interplay between technology and law.¹⁰⁶

A substantive theory of legal adaptation to technological change, therefore, differs from procedural theories in that it attempts to analyze technologies and their social impact in order to give content to the relevant regulations, however they may be promulgated. Again, this type of analysis is not immediately concerned with the roles of particular decision-makers adapting the law, nor with the procedure by which the law is adapted. While these considerations are undoubtedly fundamental in practice, substantive theories of legal adaptation to technological change simply attempt to determine whether the law should adapt to a technology, and if so, the substantive changes to the law that should be made in order to properly adapt to that technology. Questions of the proper procedure and decision-makers to carry out the adaptation are therefore a

¹⁰⁴ Cockfield, supra note 8 at 387.
¹⁰⁵ See Cockfield & Pridmore, supra note 8 at 503-505.
¹⁰⁶ Ibid at 496.
secondary, albeit important, question. Indeed, the substantive analysis might inform the choice of process or decision-makers to implement the substantive change.\textsuperscript{107}

However, despite calls for analyses of this sort, substantive theories of law and technological change are largely underdeveloped in the academic literature outside of narrow doctrinal categories.\textsuperscript{108}

Professor Bernstein does offer one instance of a substantive analysis in respect of both genetic testing and the Internet.\textsuperscript{109} She argues that both of these technologies implicate the identity interests of those affected by them, such as the way the Internet allows identity exploration and formation, or how genetic testing can reveal identity-altering facts about an individual. In her view, courts and legislators need to consider how their decisions concerning these technologies affect the identity interests of those who interact with the technology.\textsuperscript{110} Her analysis looks deeply at the meaning of identity, and how people form their lives around identity narratives that can be put under strain by their society, the law, and technologies. She also offers a way of analyzing these interests in order to assist decision-makers in determining how best to approach identity issues.\textsuperscript{111} Bernstein’s analysis is, then, perhaps the best example of a technologically-specific substantive theory of legal adaptation to technological change that looks beyond doctrinal pigeon-holes. Her analysis both offers insights into the effects of specific technologies upon individuals and society, and how decision-makers might best address those effects when raised by new technologies.

Cockfield and Pridmore offer one other example that, while useful, is incomplete. Their example concerns state surveillance and the privacy interest.\textsuperscript{112} Their analysis looks across multiple doctrinal categories and identifies a number of problems raised by increased surveillance technology, including restrictions on freedom of expression, increased discrimination, and a loss

\textsuperscript{107} The converse is, of course, also possible. The current judicial and political realities may place limits on the choice of possible substantive responses, or may require a reconsideration of the optimal legal adaptation given those realities.

\textsuperscript{108} Cockfield, \textit{supra} note 8 (“To date, there has been no attempt to develop a broader theory that transcends this compartmentalization to help us more fully understand the law” at 495).

\textsuperscript{109} Bernstein, \textit{supra} note 8.

\textsuperscript{110} \textit{Ibid} at 1039.

\textsuperscript{111} See generally \textit{ibid}.

\textsuperscript{112} Cockfield & Pridmore, \textit{supra} note 8 at 506-512.
of privacy, which they argue ultimately leads to a more unsafe state.\textsuperscript{113} Unfortunately, however, their brief analysis goes no further to investigate the specific human interests affected, nor how the law might best respond.

Substantive theories, as we have seen, find their usefulness in being responsive to specific instances of technological change, and they assist in understanding a specific technology, its social impacts, and how best we might consider those interests when responding. They tend to neglect the procedural or institutional issues, assuming existing decision-makers are capable of implementing the desired results, or at least leaving it for another time. Unfortunately, few theories of this type have been offered.

My goal in this thesis is therefore to provide an example of a substantive theory of legal adaptation in order to demonstrate the utility of this category of theory. Specifically, my aim is to develop a substantive theory that identifies some of the underlying interests affected by the technological change of the widespread adoption and use of the Internet, and to suggest how this might influence current and future development of the law.

4. Why Have a Theory of Legal Adaptation to the Internet?

The development of the Internet and digital technologies has proved to be one of the most important challenges to many disparate fields of law.\textsuperscript{114} Yet despite the academic attention given to online issues within specific areas of law, substantive theories of legal adaptation to Internet and digital technologies remain rare and underdeveloped.\textsuperscript{115} By beginning to explore legal adaptation to the Internet, the interests affected by the Internet can be identified, and decision-makers will have one more tool through which to consider legal changes.

However, when one begins a discussion of law and the Internet, one must be careful of delving too deeply into what Judge Easterbrook famously called “the law of the horse.”\textsuperscript{116} Easterbrook’s challenge to cyberlaw practitioners and students was that, like a horse, the Internet is not a body

\begin{itemize}
\item \textsuperscript{113} Ibid.
\item \textsuperscript{114} See supra note 27.
\item \textsuperscript{115} I note Gaia Bernstein’s article concerning the Internet and identity as one major exception. See supra notes 109-111 and accompanying text.
\item \textsuperscript{116} Frank H Easterbrook, “Cyberspace and the Law of the Horse” [1996] U Chicago Legal F 207.
\end{itemize}
of law, but is merely a thing to which existing bodies of law must be applied.\textsuperscript{117} In other words, just because there exist both cases about the sale of horses and cases about horses causing tortious injury, we need not develop a law of the horse. The law of contracts and torts, as they are, is enough.

Other scholars of law and technology have noted the same tendency for scholars interested in the Internet to underestimate the ability of the existing law to regulate activity on the Internet. Professor Jack Goldsmith has written that “the skeptics underestimate the potential of traditional legal tools and technology to resolve the multijurisdictional regulatory problems implicated by cyberspace.”\textsuperscript{118} While his argument focuses on the regulation of international and interjurisdictional issues, the contention that the law is often more able to adequately address new technologies within existing doctrines and categories is salient. The law can be a flexible tool, especially if judges and legislators use broad standards rather than specific rules. Indeed, where standards are written broadly enough, it’s likely that the law will never need to adapt to technological change, only be carefully implemented and construed by the courts.\textsuperscript{119} The law’s ability to keep pace should not, therefore, be underestimated.\textsuperscript{120}

While challenges to the critique of “cyberlaw” raised by Judge Easterbrook and others are certainly possible,\textsuperscript{121} I must state at the outset that my aim is not to engage in a discussion of Internet law \textit{as a field of law}. It is rather to better understand how the law within traditional legal fields has adapted in response to the Internet. As I’ve discussed, this analysis looks more generally at the relationship between individuals with respect to the Internet and the law so that we might better adapt existing legal fields to the challenges posed by the Internet. It may also assist in revealing the interests more generally protected by a legal doctrine through observation of the ways in which the law has adapted to the effects of a new technology upon those interests. I neither promote nor reject the notion that viewing the Internet as a distinct field of legal

\textsuperscript{117} \textit{Ibid} at 207-208.
\textsuperscript{119} Professor Friedman has made a similar argument. See Friedman, \textit{supra} note 2 (“If legal rules are defined in sufficient breadth, legal innovation is never necessary” at 85).
\textsuperscript{120} See Moses, “Why Have a Theory,” \textit{supra} note 33 (discussing how a theory of law and technological change can actually help avoid exaggerating the dangers posed by a new technology at 595-596).
doctrine is useful. I do, however, reject the implicit assertion that the Internet offers no challenges that require uniquely Internet-focused responses even within existing doctrinal categories. Indeed, as I will argue in Chapter 2, if the legal developments due to the rise of the Internet are to be taken as evidence, the implication is incorrect.

Examining the Internet with respect to the law is hardly new. The Internet and associated digital technologies have reshaped the legal landscape in numerous areas of law. But as I’ve argued, few analyses have attempted to look at legal adaptation to the Internet beyond individual doctrinal categories. And despite the attention paid to the Internet within doctrinal categories, the social impacts of the Internet are far from solved, and it continues to raise new legal challenges. For example, issues of online privacy remain of great concern, and many questions of how the law should, or can, respond to cyberwarfare remain unanswered. Additionally, as I will discuss in Chapter 3, virtual property and the defamation of pseudonyms remain areas that may well need to be addressed by courts and legislators in the future. The debate about whether Internet access is a human right is also ongoing, and a more complete theory of the relationship between law and the Internet will assist in determining whether Internet access deserves to be protected as a human right. A theory of law and the Internet remains relevant so long as courts and legislators continue to address its challenges, and it may well reveal the purposes of existing doctrine.

Another reason to explore the Internet is that it has now been around for some time. Many of the social impacts of the technology have been felt, and already legal adaptations have been made and tested. The Internet is in a position of ongoing development. Many issues surrounding the Internet remain to be fully addressed, yet legal developments have begun. We therefore have some wisdom of experience with the technology to draw on, even if that wisdom is far from

122 For an express articulation of the view that the Internet does not require new law, see Joseph H Sommer, “Against Cyberlaw” (2000) 15 Berk Tech LJ 1145.
123 See supra note 8.
124 See e.g. Richards, supra note 6.
125 See e.g. Dever & Dever, supra note 7.
127 Though it existed in research and military institutions long before, the Internet as we know it was made publicly available on August 7, 1991, giving it, for our purposes, an age of about twenty-five years. Old, perhaps, by modern technological standards. See Long, supra note 10.
complete. But as many issues remain to be resolved, a study of the Internet and the law will still be consequential with respect to the ongoing development of the law around the technology.

In my view, the task of examining the Internet has three primary objectives. The first of these is to begin to understand how the law has already changed in response to the Internet. This analysis must cut across doctrinal categories in order to understand the totality of legal response and its degree. As I aim for a substantive analysis, this is irrespective of whether a legal response has been made through comprehensive statutes, changes to (possibly many) existing statutes, or simply through judicial and administrative decisions. It is the totality of the impact on the law that is important rather than the specific mechanisms by which the law has been changed. Naturally, however, it will also be important to discuss the degree of change within existing doctrinal categories.

The second objective is to understand why the law has responded in the way it has. In this, attention must be given to the common themes of the legal responses. A substantive theory of law and the Internet entails an analysis of the kinds of challenges to the law created by a new technology, and how the law has attempted to respond to those challenges. Such an analysis will look at the five categories discussed earlier in this Chapter, and discuss, for example, whether new harms have arisen, or whether the law is responding to a change in an existing legislative balance. In other words, this analysis must address the relationship between the law and the technology to understand why the law had to change.

The third objective is to better understand the social and human impacts of the technology itself. The law, ideally, is responsive to the real harms and impacts faced by members of a society. Thus, where it has responded, there may be an opportunity to better understand the underlying issues affected by a technology, and thus, how a technology interacts with people to improve or harm their lives, or how it might change the balance between winners and losers in a society.

Based upon the above analyses, the fourth objective of analyzing the legal responses to the Internet is to suggest an application for these findings to other areas of law, and articulate a forward-looking theory of legal responses to the Internet. If there are new harms, are new

---

128 See Subsection 2.1, above.
remedies needed? Does the balance of existing legislation need to be changed, or are there distributive reasons to alter the law? Where can we extend the law to cover the observed shortcomings? As I will argue in Chapter 3, the interests affected by the Internet do indeed have effects that may require new legal adaptation in a number of legal categories.

But while legal adaptation may be warranted in response to a technology, it does not follow that such technology-focused laws should be construed as a single, internally coherent body of law. Instead, where new law or legal changes are required, in most cases, these technology-specific laws should be created within the confines of established areas of law. This does not preclude the possibility that new areas of law may arise as a result of the study of a technology, but the argument made in this thesis does not demand it.

Indeed, despite concerns about being drawn into the “law of the horse,”\textsuperscript{129} even a cursory review of current and future technologies will show that, with respect to some technologies, there are few existing legal principles that one can apply and an entirely new set of laws needs to be created. For example, technologies related to human reproduction, including issues of \textit{in vitro} fertilization\textsuperscript{130} and genetic testing,\textsuperscript{131} have required new laws and regulations. Canada’s \textit{Assisted Human Reproduction Act}\textsuperscript{132} is an example of an entirely technology-focused law. Artificial intelligence and human cryogenics, should they ever exist, will undoubtedly require new law, even if that law is as simple as an outright ban.\textsuperscript{133}

Therefore, it is not going too far to suggest that a principal benefit of a theory of legal adaptation to the Internet is to offer changes or additions to the law that reflect the observed impacts of the Internet. By developing this theory, we may find better ways to regulate, control, or allow technologies, and we may better understand how to respond when new issues arise in respect of them.

5. Methodology for Producing a Substantive Theory

\textsuperscript{129} Easterbrook, \textit{supra} note 116.
\textsuperscript{130} See Moses, “Why Have a Theory,” \textit{supra} note 33 at 591-593.
\textsuperscript{131} See Bernstein, \textit{supra} note 8.
\textsuperscript{133} See Friedman, \textit{supra} note 2.
My proposed methodology for developing a substantive theory of legal adaptation to the Internet is partly empirical and partly interpretative. I take as my subject the legal responses of the past to the Internet in order to offer a theory for the present and possibly the future. I am not the first to suggest this process. Professor Cockfield asserted that:

The discrete categories [of law] could inform a law and technology theory, which in turn could reflect back onto these disciplines and provide scholars with a broader perspective to promote a fuller understanding of their areas of study.134

Cockfield did have in mind a theory of law and technology more generally, while my focus is somewhat narrower, considering only the Internet. By focusing on a single technological universe, albeit on without well-defined boundaries, my aim is to reveal the deeper concerns that engender the responses to that particular technology. However, caution must be taken not to overstate the potential utility of the analysis. This is, as Cockfield notes, merely “one more tool within a scholar's methodological toolbox to promote more fully informed legal analysis.”135

Cockfield & Pridmore have also provided a methodology for how such a substantive theory can be arrived at. They described the steps as follows:

Part 1

Determine whether the technology change is undermining traditional interests by:

A. Identifying the traditional interest protected by law (e.g., business certainty, protection of innovator's rights) by resorting to traditional doctrinal analysis applicable to the affected area of technology law; and

B. Assessing whether the interest is being unduly disrupted by technology change.

[…]

Part 2

If the first part of the analysis determines that technology change is disrupting traditional interests, the next step is to use more contextual analysis that:

134 Cockfield, supra note 8 at 387-388.
135 Ibid at 387.
A. Scrutinizes the broader context of technology change and its potentially unanticipated adverse outcomes for the traditional interest as well as for other protected interests the law seeks to protect; and

B. Seeks to find legal solutions to protect the traditional interest that are less deferential to precedent and traditional doctrine.¹³⁶

Thus, in their view, the question is first whether an interest already protected by law is implicated and adversely affected by technological change. Only then should the analysis continue to attempt to determine how the technological change might be injuring the protected interest, and how best to go about remediating the injury. This method is clearly designed to assist decision-makers such as courts and legislators in determining how best to respond to a new technology.

However, the analytical structure they suggest is not incompatible with my project. My aim is to investigate the past legal responses to the Internet in order to better understand the interests being affected. Thus, Part I of their analysis is germane. However, I disagree with their focus only on those interests that are already legally protected. As I argue in Chapter 2, in some cases, technology may create new harms and lead to the identification of new interests that either may have previously not have been explicitly recognized by the law. The analytical procedure of Cockfield and Pridmore will leave out the identification of new interests and the development of potentially new rights by looking only to those interests already protected. I therefore will attempt to look at all affected interests, even those that might previously have been unrecognized by the law.

In looking only at legal responses to technology, my approach begins in expressly legal terms, and differs from others that could be considered. For example, I do not begin with sociological approaches and research on the Internet,¹³⁷ rather taking the legal responses as my primary source of empirical evidence concerning the underlying interests affected by the Internet. Despite this, sociological accounts will be used to better understand the possible rationales behind a given legal response to the Internet. Additionally, my approach does not engage in a sophisticated technical analysis of the Internet and its functions and uses in relation to the law.

¹³⁶ Cockfield & Pridmore, supra note 8 at 503-505.
¹³⁷ For a number of sociological (as well as legal) views of the impact of the Internet on society, see Kerr, Steeves, & Lucock, supra note 14.
This latter approach is, in my view, unfortunately prone to obfuscating the underlying human interests rather than revealing them.\textsuperscript{138}

My approach can thus be summarized as follows. First, I identify a number of doctrinal categories that have seen legal adaptation in response to the Internet, and examine the types of challenges that led to the legal response using the categorization scheme discussed earlier in this Chapter. This examination should elucidate the degree to which the Internet poses challenges for various areas of the law.

Secondly, by using the analysis from the first part, I attempt to find themes in the legal responses that suggest an underlying interest being affected by the technology. The categorization from the first part will help determine the similarities and differences between the legal responses, as well as the degree to which the underlying interest may have been affected. Because any one of these themes could be the subject of a separate theory, I will focus on only one such theme in order to better understand the way in which the technology interacts with the interest, which is in this case the identification of personhood interests in Internet use. Developing this theme will both demonstrate the utility of substantive theories of legal adaptation to technological change as well as offer insight into the nature of the Internet and legal responses itself. While it’s possible that different themes could be in conflict with each other, as I will only focus on one such theme, such a consideration is outside the scope of this thesis. However, it remains a potential ground of contention on which to challenge the results of this method should such a conflicting theme be found.

Thirdly, I will closely examine the nature of the legal responses and adaptations to the Internet implicated within the common theme to understand precisely how the technology has affected the underlying interest. This assumes that the legal responses reflect a concern for an underlying interest, or multiple interests. While an analysis of whether the aim of legal adaptation is to protect the interests of the polity to which it applies is outside of the scope of this thesis, I acknowledge that this could be a weakness of this approach. However, I do not believe it

\textsuperscript{138} Copyright law is one area where the technical dimensions of the interaction between the law and the technology have overshadowed the core concerns beyond the law itself. See e.g. \textit{MAI Systems Corp v Peak Computer, Inc}, 991F (2d) 511 (9th Cir 1993) (in which the United States Court of Appeals for the Ninth Circuit concluded the loading a copyright-protected work into the random-access memory of a computer constituted an infringing copy).
unreasonable to assume that the law and legal adaptations are responsive to the interests of the people to which they apply and are presumably designed to protect.\textsuperscript{139} Therefore, by closely analyzing the legal responses, their stated purposes, and additional sociological, economic and philosophical research related to the technology, my aim is to elucidate precisely the relationship between the technology, the affected interests, and the legal responses. It should be noted that the stated purposes of a legal adaptation, if there are any, will not be determinative of the true purpose of the response. Indeed, in my view, the underlying concerns may well not be properly identified, or they may simply be couched in legal doctrine that does not attempt to understand what interests are affected.\textsuperscript{140} This will form the central part of the analysis, and will result in the production of a substantive theory of legal adaptation to the Internet.

Finally, I will take the theory developed in the third step, and apply it to some areas of future legal development concerning the Internet. By having identified both the underlying interests being affected, and the way in which the Internet affects those interests, the theory will assist in developing legal responses to potential areas of future challenges posed by the Internet. By understanding how a technology affects certain interests and how people interact with a technology, we can better craft laws to ensure that the purpose of the legal adaptation is achieved without undue consequences. As I will argue in Chapter 3, this theory may also suggest new challenges to the law that may not have been fully dealt with previously.

There are at least three major challenges to applying my approach more broadly to other technologies. The first of these is the observation that in order to analyze past instances in which the law has responded to a given technology, there must be past instances to analyze. While there are certainly many such instances with respect to the Internet, some of which are discussed in Chapter 2, this methodology is of little utility when courts or legislatures are first faced with issues created by a new technology. I note this only a concern because it is my aim to

\textsuperscript{139} See e.g. \textit{Jones v Tsige, supra note 77} (in which a harm without a remedy led to the creation of a new tort in Ontario).

\textsuperscript{140} For example, despite privacy rights being recognized by the courts, precisely what interest privacy rights reflect is still debated. See e.g. \textit{R v Spencer}, 2014 SCC 43, [2014] 2 SCR 212 (in which the Supreme Court of Canada attempts to determine why online anonymity is important at paras 41-49); Jonathan Khan, “Privacy as a Legal Principle of Identity Maintenance” (2003) 33 Seton Hall L Rev 371 (reviewing the history of the view of privacy as related to identity issues at 378-383); Lisa Austin, “The Privacy Interest in Anonymous Blogging” in Dan Hunter et al, eds. \textit{Amateur Media: Social, Cultural and Legal Perspectives} (New York: Routledge, 2013) 208 [Austin, “Anonymous Blogging”].
demonstrate the utility of this kind of analysis for not only the Internet, but other technologies as well. Therefore, my approach may well be insufficient to assist in these circumstances. Nonetheless, this approach is useful insofar as it demonstrates that, in certain cases, existing law may not be able to fully address the challenges raised by a new technology. The categorization structure for types of challenges raised by new technologies that I reviewed earlier in this Chapter may also assist decision-makers in understanding the ways in which the law may need to adapt. Additionally, implicit in my methodology is the imperative to attempt to understand both the underlying interest affected by the technology and how the technology impacts that interest in order to properly craft the necessary legal adaptations. However, as I’ve discussed above, there is also certainly merit in waiting until a more complete analysis can be carried out. Rushed laws that prove poorly tailored to the circumstances may be worse than no action at all.\footnote{141} 

A second problem may be that analyzing the legal responses to technology might lead to inaccurate conclusions about the underlying interests. It’s possible, after all, that a given legal adaptation was inaptly made. Where a legal response incorrectly identified an interest, or where its response failed to properly respond, using that response as evidence of an underlying interest could lead to incorrect results. This could be a result of a simple error to make the proper or necessary changes. It could also be the result of the decision-making body using the spectre of technological change in order to enact that decision-maker’s agenda,\footnote{142} or it might be the result of political pressure from special interests to change the law in a way beneficial to them. In these cases, an analysis using the method proposed here might not only reach erroneous results, but might actually find an underlying interest that corresponds to the enacted agenda of either the decision-maker or the special interest, rather than the interests that might actually be affected by a technology. In other circumstances, a legal response may also fail to disclose a single clear interest at stake, instead identifying multiple interests. This may lead to multiple possible interpretations,\footnote{143} or it may lead only to confusion.

\footnote{141}{See Moses, “Agents of Change” \textit{supra} note 22 at 768.}
\footnote{142}{See Price & Duffy, \textit{supra} note 87 and accompanying text.}
\footnote{143}{Copyright law provides an example in the conflicting views surrounding the interests protected. Some commentators favour a view of copyright as protecting authorial autonomy and elements of self-expression, while others see it as a purely economic right. See e.g. Neil Netanel, “Copyright Alienability Restrictions and the Enhancement of Author Autonomy: A Normative Evaluation” (1993) 24:2 Rutgers LJ 347 (favoring the autonomy interest); William M Landes & Richard A Posner, “An Economic Analysis of Copyright Law” (1989) 18:2 J Leg Stud 325 (favoring the economic interest).}
While it’s impossible to fully address this issue, in my view, as this analysis attempts to find common themes amongst adaptations made across multiple doctrinal categories, the analysis should only be inaccurate where most of the connected legal adaptations were inaptly made. Additionally, by considering the academic literature on each such adaptation, it should be possibly to identify where perhaps an adaptation is seen as inapt or unresponsive to the motivating interest. In cases where the legal adaptation is a response to political pressure from special interests, hopefully that influence can be discerned and considered when analyzing that adaption. In most cases, I expect, the potential moneyed and influential interests responsible for influencing a particular adaptation should be clear. The academic literature may also assist in identifying any outside influences and sorting multiple possible interpretations to find those that best explain the response.

The third challenge is that my analysis may miss instances in which an adaptation was considered, but it was determined that no response was necessary or desirable. Taking account of such instances may assist in ruling out possible underlying interests affected by a new technology, or in better understanding what degree of impact warrants a legal response. While I attempt to consider instances of court decisions where legal adaptation was considered and rejected, they are not my focus, nor will it be possible to find all such instances where the decision-makers were government officials or administrators. However, this oversight will be of limited consequence where the legal adaptations that have occurred paint an accurate picture of the affected interests and the rationale for the adaptation.

Thus, in my view, despite these potential shortfalls, the analysis will be useful in addressing future legal challenges and will at least contribute to a better understanding of the Internet. Naturally, a substantive theory of this type can never claim to be complete, and I do not propose to produce anything more than what Cockfield has referred to as “one more tool within a scholar's methodological toolbox.” I only claim that exploring past legal responses to the

144 For example, in Intel Corp v Hamidi, the California Supreme Court considered, but refused, granting a real property right in computer servers for the purposes of trespass law in order to provide a legal recourse against email spam: Intel Corp v Hamidi, 30 Cal 4th 1342, 71 P 3d 296 (Cal Sup Ct 2003) at 49-50.
145 Cockfield, supra note 8 at 387.
challenges raised by the Internet will offer some insight into the nature of the relationship between technology, society and the law.
Chapter 2
The Internet and the Rise of Digital Rights

1. Chapter Overview
This Chapter examines legal adaptations to the rise of the Internet following the process outlined in Chapter 1. I begin by very briefly reviewing some of the legal challenges created by the Internet across a number of doctrinal categories and the responses or adaptations made by the law and legal institutions. These categories include property and trespass, cybercrime, cyberwarfare, contract and commerce, copyright, privacy, defamation and freedom of expression, and commercial spam messaging. While this review is far from exhaustive, a number of legal adaptations and reactions to the Internet suggest that many legal adaptations to the Internet are responsive to an internal and personal experience of the Internet by its users. These adaptations appear to respond to the interaction between the Internet and the personhood interests of its users. That is, the legal adaptations to the Internet are not solely reactive to the surface impacts of the Internet as a ubiquitous and fairly cheap method of mass communication and copying, but are also aimed at the distinctive capacity of the Internet to function as a non-geographical “space” in which people interact, express themselves, develop their identities, and grow as people. It’s also responsive to the ways in which individuals can become harmed in this space, and the singular opportunities available for abuse and assault. As such, the Internet gives rise to “digital rights,” which are rights that are either unique to the online space, or which are especially extended in that arena. I then examine a number of identified legal adaptations in greater detail to demonstrate the particular Internet personhood interests being addressed by the law, including within the areas of privacy, defamation and freedom of expression, and email spam. The implications of this are further explored and developed in Chapter 3 to produce a substantive theory of legal adaptation to the Internet.

2. A Brief Review of Legal Adaptations to the Internet
   a. Property and Trespass
The notions of property and trespass are difficult ones to apply in the context of the Internet. Certainly there is property in the physical apparatuses that allow for the Internet to function, including the communication infrastructure that allows information to flow electronically, and the computer equipment that stores information, directs and relays information, or is used to access that information.\footnote{For a more thorough overview of the basic structure of the Internet, see Patricia L Bellia et al, \textit{Cyberlaw: Problems of Policy and Jurisprudence in the Information Age}, 4th ed (St. Paul: Thomson Reuters, 2011) at 16-24.} This equipment, which comprises the totality of the physical structure of the Internet, would typically be described as chattels. They are things that can be owned, but they are not real property. However, despite the fact that the Internet consists of a vast, connected array of physical hardware owned by numerous parties and located in jurisdictions around the world, the Internet is often characterized as a \textit{virtual} place that can be visited, entered, and explored by its users. Indeed, Dan Hunter has catalogued the inherent tendencies of people to label aspects of Internet use with terminology derived from physical space.\footnote{Dan Hunter, “Cyberspace as Place and the Tragedy of the Digital Anticommons” (2003) 91 Cal L Rev 439 at 453-454.} He refers to it as the metaphor of cyberspace, and warns that treating cyberspace like a place can be highly problematic for the continuing function of the Internet.\footnote{See generally \textit{ibid}.}

But the metaphor of cyberspace as a place is apt, because it often \textit{feels} like a place to its users, as Hunter acknowledges.\footnote{\textit{Ibid} at 443, 452.} This has profound effects not only upon the way in which the Internet is used and how it affects human interaction, but also upon the law.

An example of these challenges can be seen in the questions concerning how to regulate unauthorized access and use of privately-owned computer systems or networks that are otherwise open to Internet traffic. The facts of \textit{eBay Inc} v. \textit{Bidder’s Edge, Inc.} are illustrative of this issue.\footnote{\textit{eBay Inc v Bidder’s Edge, Inc}, 100 F Supp (2d) 1058 (ND Cal 2000).} eBay.com was, and is, a popular website that features auctions for items posted by its users and retailers. Bidder’s Edge operated a service (AuctionWatch.com) that allowed its users to search for auctions across a number of different websites, including eBay.com, with a single query. In order to aggregate the information of multiple auction-hosting websites, Bidder’s Edge employed automated software, called “bots,” that would access these auction sites, including eBay, and obtain their auction information.\footnote{\textit{Ibid} at 1060-1062.} While these software bots did nothing that an
individual person could not do on eBay, and thus utilized only systems available to the public, the automated nature of the bots meant that they could make information requests to eBay’s servers many times faster than a human, and thus utilize more of their server capacity. eBay brought suit against Bidder’s Edge to obtain an injunction preventing this automated use of eBay’s servers, arguing that Bidder’s Edge was committing the tort of trespass to chattels. While the cause of action was trespass to chattels, in reality, eBay’s interest in bringing the suit was almost certainly to protect the use of their information, in which they had no enforceable rights, rather than the use of their network infrastructure. The claim of trespass to chattels was, in all likelihood, just a convenient way of attempting to control the third-party use of their information though other means. Nonetheless, in deciding the case, the United States District Court for the Northern District of California set out the test for trespass to chattels with respect to a computer system as follows: "(1) defendant intentionally and without authorization interfered with plaintiffs possessory interest in the computer system; and (2) defendant’s unauthorized use proximately resulted in damage to plaintiff." Ultimately, the Court decided that this test was met because the defendant had used the limited resources of the plaintiff without authorization (and damage was therefore imputable), and granted the injunction sought.

If we’re to categorize the challenge raised by the Internet here using the scheme developed in Chapter 1, this would appear to fall under the third category for bringing about new harms or new ways of inflicting harms. However, this assumes that Bidder’s Edge has inflicted a harm on eBay to begin with. As Dan Hunter points out, the Court’s finding is reliant on the view of cyberspace as place. The identified harm was the use of server capacity and bandwidth. However, there is no possessory interest in these things, only in the physical servers themselves. In order to find interference with a possessory interest, the Court had to conflate the server capacity and bandwidth with the physical chattel itself. This, Hunter argues, is ultimately a result of the conflation of trespass to chattels with trespass to land, as the court downplayed the requirement of the former tort to involve damage to the chattels, whereas trespass to real

152 Ibid at 1063-1065.
153 Ibid.
154 Ibid at 1069-1070.
155 Ibid at 1073
156 Hunter, supra note 2 at 484-487.
157 eBay Inc v Bidder’s Edge, Inc, supra note 150 at 1071.
property requires no such damage.\textsuperscript{158} If one views the action of Bidder’s Edge purely through a physical and technological lens, all they had done was send and receive data in accordance with the basic protocols of the Internet. eBay’s servers were as much a part of this exchange as the bots employed by Bidder’s Edge. One could analogize it to a telephone call that was picked up by eBay’s servers, from which no liability for trespass to chattels would presumably follow.\textsuperscript{159} However, by viewing the exchange through the metaphor of place, the Court construed the bots as an unauthorized “access” that used up a form of limited spatial capacity in bandwidth and server capacity. Thus, a harm was found.

In the later case of \textit{Intel Corp v Hamidi},\textsuperscript{160} the California Supreme Court faced a similar issue where the tort of trespass to chattels was raised. In that case, the alleged trespass resulted from unsolicited emails sent in bulk to employees of Intel by a disgruntled former employee. As these emails crossed Intel network systems and ended up being accessed by Intel computer systems, Intel claimed that it was a trespass to chattels.\textsuperscript{161} Here, the Court disagreed, though not because its conception of trespass differed from that of the decision in \textit{Bidder’s Edge}. It merely found that Intel could show no actual damage to its chattels, the real harm being from the content of the emails and the loss of productivity from employees reading them, for which there was no liability.\textsuperscript{162} However, the Court noted that, in future cases, if the volume of unsolicited emails sent is sufficient to impair the function of computer or network systems, the tort may be available.\textsuperscript{163}

As these cases demonstrate, the notion of the Internet as a place that can be explored is a powerful one, and it has raised a number of conceptual challenges for the law concerning the limits and applicability of the notions of physical property and trespass.\textsuperscript{164} Virtual property,

\textsuperscript{158} Hunter, \textit{supra} note 147 at 486-87.
\textsuperscript{159} Bellia et al, \textit{supra} note 146 (commenting on this case and suggesting that making a call to someone who answers, even if unsolicited, would unlikely be a trespass to chattels by virtue of requiring the use of the recipient’s phone or phone system to complete the call at 33).
\textsuperscript{160} \textit{Intel Corp v Hamidi}, \textit{supra} note 144.
\textsuperscript{161} \textit{Ibid} at 37-38.
\textsuperscript{162} \textit{Ibid} at 41.
\textsuperscript{163} \textit{Ibid} at 43-44.
which is rivalrous property within virtual worlds such as video games, also raise questions of whether property can exist in things only experienced as property, but physically composed of nothing more than electronic bits.\footnote{See Fairfield, “Virtual Property”, supra note 15.} It’s clear that there is value in virtual property,\footnote{For example, Ailin Graefe became the first real world millionaire through the sale of virtual property assets in 2006 by selling virtual property in the online game \textit{Second Life}. See Rob Hof, “\textit{Second Life}’s First Millionaire”, \textit{Bloomberg Businessweek} (26 November 2006), online: \url{http://www.businessweek.com/the_thread/techbeat/archives/2006/11/second_lifes_fi.html}.} but it’s very unclear whether there are, or should be, property rights associated with it.\footnote{For differing views on whether virtual property should be legally recognized, see Lawrence, \textit{supra} note 15 (arguing against legal recognition of virtual property); Fairfield, “Virtual Property”, \textit{supra} note 15165 (arguing in favour of legal recognition for virtual property).} Whether the arguments for either side are persuasive is likely to be dependent on whether one takes an “internal” or “external” view of the Internet.\footnote{Bellia et al, \textit{supra} note 146 at 32.} The external view sees the Internet only as composed of physical infrastructure and a number of electronic functions that moves data efficiently about. However, the internal view sees the Internet from the perspective of the user, and relates to the experience the user encounters on the Internet rather than its technical parts.\footnote{\textit{Ibid.}} From the former view, the notion of virtual property appears ludicrous, as it’s nothing more than transient electronic data governed by mutable software systems. From the latter perspective, legal protection of virtual property appears rational, as virtual property can seem as real as physical chattels to users, and can exhibit many of the same properties, such as being rivalrous.

Legal adaptation to recognize virtual property remains prospective, however. And despite the importance of the decisions discussed above concerning trespass to chattels for our understanding of legal responses to the Internet, these decisions represent only limited legal adaptation. As discussed in Chapter 1, they merely decide whether existing law is applicable. They neither create new law nor truly modify the content of existing law.

However, at least one area of property ownership online has seen considerable legal adaptation. Domain name ownership has become a hotly contested arena, especially with regard to the use of existing trademarks as a domain name and the law has had to respond. The problem is clearly illustrated in \textit{Brookfield Communications, Inc. v. West Coast Entertainment Corp.}, in which the United States Court of Appeals for the Ninth Circuit determined that trademark law granted a
trademark owner injunctive relief against an organization that had used its trademark in an Internet domain name registration.\textsuperscript{170} The case concerned a video rental store, West Coast, which had registered the domain name “moviebuff.com.” “MovieBuff” was a registered trademark of Brookfield Communications, who then brought suit against West Coast for a preliminary injunction prohibiting their use of the domain name. The Court ultimately granted the injunction, finding that there was a likelihood of consumer confusion in the use of a domain name by one organization that is a trademark of another.\textsuperscript{171}

Returning to the classification scheme from Chapter 1, the legal problem created by domain names is one of both creating a new method to inflict a harm (in this case consumer confusion) and a requirement for coordination, as domain names must be unique and operate as the principle resource locators for Internet users.

In order to resolve both issues, it was necessary to empower an organization with the ability to both promulgate rules for domain name disputes that are responsive to trademark interests, but would also work with registrars and ROOT servers to ensure that the domain name system continued to operate.\textsuperscript{172} It would also have to take into account the interests of the technical community, internet service providers, and users. The eventual result was the creation of the Internet Corporation for Assigned Names and Numbers (ICANN).\textsuperscript{173} ICANN largely took over the administrative functions for the domain name system previously performed by the US government and American academics, and it was the US government that both proposed and ceded power to ICANN.\textsuperscript{174} While ICANN has no direct statutory or legal authority, the cession of power to a non-profit organization by the US government does represent a form of legal adaptation insofar as the legal order concerning domain names clearly changed. Indeed, the Uniform Dispute Resolution Policy (UDRP), which was created by ICAAN and governs many top-level domain name disputes, can easily be seen as a form of non-state law.\textsuperscript{175} While not authorized directly by a state law, the \textit{de facto} power of ICANN, its dispute panels, and

\begin{itemize}
\item\textsuperscript{170} Brookfield Communications, Inc v West Coast Entertainment Corp, 174F (3d) 1036 (9th Cir 1999).
\item\textsuperscript{171} Ibid at para 72.
\item\textsuperscript{172} See Post, supra note 61 at 148-158.
\item\textsuperscript{173} Ibid.
\item\textsuperscript{174} Ibid.
\item\textsuperscript{175} Ibid at 158-161.
\end{itemize}
cooperating registrars and registry services, gives the UDRP nearly perfect enforceability.\textsuperscript{176} This kind of propertization of non-real virtual assets necessarily takes an internal view of the Internet. Propertization of digital locator elements within an electronic system of this sort is difficult to reconcile in an external view as it’s not clear what, exactly, is being valued. Only by understanding the experiential aspects of the Internet can one appreciate the importance of domain names, and thus give them their appropriate value.

While there are likely many other examples of legal responses to the Internet within the realm of property, this review is sufficient to demonstrate that notions of property and trespass have been challenged by the Internet, and that the response to those challenges can largely depend upon the perspective of the Internet (internal or external) taken by decision-makers.

b. Cybercrime

Cybercrime is an umbrella term that encompasses a wide variety of law and criminal action. Because of its scope, we will look at only a small sampling of issues arising from the Internet with respect to criminal law.

Professor Susan W. Brenner identifies three principle types of crimes that might fall under the umbrella of cybercrimes:

(1) A computer is the target of a crime (often a new cybercrime); (2) a computer is a tool used to commit a traditional crime such as theft or fraud; and (3) a computer plays an incidental role in committing one or more crimes.\textsuperscript{177}

I will address these categories briefly in turn, discussing in the second category also cases where a computer is used as a tool to commit a harm to persons or property, rather than computer systems.

The first category is that of crimes in which computers are the target. These include “hacking,” dedicated denial of service attacks (DDoS), and the development, spread and use of malware,

\textsuperscript{176} The decisions of dispute resolution panels can be directly enforced by the registries simply by changing the IP address associated with the domain name. \textit{Ibid.}

viruses, or worms to damage or inhibit the use of computer equipment. These types of conduct raise particular challenges for the law, because, not only are they unique methods of committing harms, the harms themselves can be considered somewhat new. While it is possible for many of these computer-targeted crimes to have physical effects, in most cases, the harm is the denial of the use of a computer system or network by otherwise authorized users. The harm here largely arises from the modern societal reliance on computer systems for basic productivity functions and commercial transactions. Disruption therefore leads to economic losses, such as lost productivity, and expenditures in repairing the infected computer systems to working order. The newness of the harm, or at least the method of achieving the harm, is evidenced by the initial lack of criminal law that applied to the infliction of harm through these means. Numerous new criminal laws have therefore been created in both Canada and the US to respond to these activities. Perhaps most notable, and controversial amongst these, is the Computer Fraud and Abuse Act in the United States. The relatively short statute prohibits access to

---

178 Some explanation of these terms may be necessary. “Hacking” generally refers to gaining unauthorized access to a computer system, and possibly obtaining data from the system, or deleting, modifying, or adding the data present there. A “DDoS” attack is a primitive form of Internet-based attack that uses a high volume of requests to a networked-connected server or computer system to overwhelm that system’s ability to process such requests with the goal of disabling it or denying others the use of it. In this, no direct “access” to the targeted system is necessary. A “virus” is a piece of software that invades host computers attached to normal computer files, where it can replicate and attach itself to other files in order to spread to other computers when transferred. A virus requires human action for it to replicate, such as the copying or sending of an infected file. Virus programs can have many effects upon host computers, depending on their design, including modification of data, disabling the computer, or sending information from a computer back to the virus creator. A “worm” is like a virus, but can replicate and transmit itself without human action. These can spread very fast, and can often overwhelm networks with the sheer number of transport requests generated by their software. “Malware” is an umbrella term that includes viruses and worms, as well as any unwanted software that executes upon a computer system. Malware is often used to refer to spyware or adware, the former of which covertly sends data from the host computer back to a specific location, while the latter serves to display unwanted advertisements upon the host computer. See ibid at 16-56.

179 For example, the Stuxnet worm was most likely created by the Israeli and American governments to infect the software controlling Iranian nuclear enrichment facilities. The worm would cause physical damage to the centrifuges used in uranium processing by causing them to speed up beyond their structural capabilities. See David Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," The New York Times (1 June 2012), online: The New York Times <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=2&pagewanted=2&seid=auto&smid=tw-nytimespolitics&pagewanted=all>; Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," (11 July 2011), online: Wired <http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1>.

180 Brenner, supra note 177 at 38-39.

181 Ibid at 21.

182 See e.g. Computer Fraud and Abuse Act, 18 USC § 1030 (2012) (American criminal law dealing with a wide variety of computer related crimes); Criminal Code, supra note 44, ss 342.1-342.2 (Canadian criminal law prohibiting unauthorized use of a computer).

183 Computer Fraud and Abuse Act, ibid.
“protected computers,” which, while ostensibly originally limited to computers used by the US government, financial institutions, or used in interstate trade, has effectively become expanded to include most computers, including cell phones. The Act’s few provisions generally prohibit almost any unauthorized access to a protected computer, and because of the vagueness of the meaning of the term “without authorization,” it might well criminalize millions of activities carried out by Internet users every day. Professor Brenner points out that many of the laws in the US created to respond to these new forms of harmful conduct, including the Computer Fraud and Abuse Act, were premised upon traditional trespass laws, which may go some way to explaining its focus on lack of authorization and its very broad and vague prohibitions. It also again suggests that legal responses to the law, even in the criminal context, cannot escape the metaphor of cyberspace as place.

Computer-targeted crime is therefore one of the most clear-cut examples of a challenge to existing law created by the Internet in the form of new means of inflicting harms, and the corresponding response has generally been the creation of new laws. However, the second class of cybercrime, in which computers are merely tools to commit crimes or harms targeting persons or property, can become murky. This may seem counter-intuitive, as in many cases, the conduct considered requires no new laws. A threat delivered by email is little different from one delivered by the regular mail, and a fraudulent misrepresentation on a website is functionally the same as one in a newspaper. Where this class of cybercrime becomes difficult are those situations in which it’s unclear whether any existing law applies to a new situation created by the Internet. For example, can someone be prosecuted for “stealing” computer services, such as leeching off of a neighbour’s unsecured wifi? Is hacking into an online casino to modify the

---

184 Ibid, § 1030(e)(2).
186 Ibid.
187 Brenner, supra note 177 at 22-24.
188 The Internet may raise unique challenges with respect to the enforcement of these laws due to jurisdictional issues or the problem of identifying the person who committed the crime when they hide behind anonymity. However, we are not immediately concerned with these issues, and anonymity will be addressed at length later in this Chapter.
189 It is possible that this could be prosecuted in Canada under subsection 342.1(1) of the Criminal Code, which provides that:

“Everyone is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years, or is guilty of an offence punishable on summary conviction who, fraudulently and without colour of right,

(a) obtains, directly or indirectly, any computer service;
software such that it’s much more likely for players to win a form of theft or fraud if the hacker did not attempt to achieve a gain? One question that has perhaps been answered is the question of whether the unauthorized copying of data from a computer system can be theft. In *R v Stewart*, the Supreme Court of Canada held that the taking of confidential information cannot be theft as there is no deprivation. Information cannot be stolen, since it is non-rivalrous and the original holder of the information cannot be said to have been deprived of that information.

While this decision did not concern computer data, it seems equally applicable to unauthorized data copying on a computer.

One area in which Canadian law has clearly adapted to a harm carried out by Internet technology is that of revenge porn. A relatively recent *Criminal Code* enactment specifically targets the sharing, publication, distribution, sale or transmission of intimate images of a person without their consent. The provision follows considerable news attention paid to cases in which, typically, an ex-boyfriend posts nude or sexual images of a woman taken in confidence. While revenge porn can exist without the Internet, the Internet has allowed it to proliferate with ease. The revenge porn statutes enacted in Canada, as well as in multiple US states, therefore represent a legal adaptation to a harm facilitated by the Internet but affecting well established

---

(b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system […]"

However, no cases appear to address this issue. See *Criminal Code*, supra note 44, s 342.1(1).

190 Professor Brenner discusses the real world case in which an anonymous hacker changed the software of an online casino to make it easier for any player to win. The casino paid out 1.9 million dollars before it was corrected. The hacker was never caught. However, if this hacker made the modification without any intent or action to profit himself, could this be construed as fraud or theft? The issue is unclear. See Brenner, supra note 177 at 58-61.


192 *Ibid* at 35.

193 *Criminal Code*, supra note 44, s 162.1. The Act amending the *Criminal Code* to include the provision was the *Protecting Canadians from Online Crime Act*, SC 2014, c 31.


195 For example, Hustler Magazine was successfully sued in 1984 for publishing a stolen nude photograph of a woman that was submitted to the magazine with a forged consent form. *Wood v Hustler Magazine, Inc*, 736 F (2d) 1084 (5th Cir 1984).

196 For a complete list of states with revenge porn laws, see Cyber Civil Rights Initiative, “31 States Have Revenge Porn Laws,” online: <http://www.cybercivilrights.org/revenge-porn-laws/>.
interests in privacy and reputation. It is also a clear case of new law being created to address a new manner of committing a harm to an individual.

Finally, the last category of cybercrime is that of crimes in which a computer or the Internet is only incidental to the crime being committed. Here we are less likely to find direct legal adaptation within the criminal law, as by and large, existing law is sufficient to address the crime. A criminal may plan a murder by doing research on the Internet, or a drug dealer might communicate with his clients by email. In these cases, the nature of the Internet itself matters little. Often these crimes are regularly committed in the Internet’s absence, and the crime reveals little to differentiate the Internet from other technologies such as the telephone or books. Therefore, there is little reason to analyze these issues in depth. Any legal challenges posed generally relate to the gathering of evidence and the investigation of the crime, rather than the commission of the crime itself. While legal adaptations in these areas are important with respect to privacy and search and seizure laws, I will examine those later when looking at privacy more generally.

Legal responses to the Internet within the criminal law is a broad topic, and one that cannot be adequately surveyed here. However, this brief review does demonstrate that the Internet has given rise to numerous new challenges to the criminal law, and a number of new laws have been created in response.

**c. Cyberwarfare**

Cyberwarfare remains a burgeoning field of law. As international bodies of law, international humanitarian law (IHL) and the law of armed conflict (LOAC) are somewhat slow to respond to technological changes. No treaty dealing with cyberwarfare exists, and there is a dearth of decisions of international courts considering the challenges raised by cyberwarfare. It will likely require major publicly-acknowledged international cyberwarfare events before there are any such decisions. However, that is not to suggest that cyberwarfare raises no new challenges for IHL or LOAC. Indeed, it raises a great variety of them. Here, I can address only a few.

---

Most of the challenges to IHL and LOAC stem from the vague wording used in treaties and international documents when outlining the rights of nation-states in international conflict. One of the most pressing questions with respect to cyberwarfare is the whether a state is entitled to respond with force to a cyberattack. The *Charter of the United Nations* generally prohibits any use of force by a nation state against another.198 However, Article 51 of the *Charter* states that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations."199 In the absence of other use of force provisions in the UN *Charter*, this right to self-defence is the only occasion on which a state can legally use force against another sovereign state without a Security Council resolution. Thus, the question is whether a cyberattack can be an “armed attack.” Unfortunately, politicians of the time did not anticipate this problem. Indeed, the Foreign Relations of the US Senate stated that the term “armed attack” is “ordinarily self-evident,” and that “there is rarely, if ever, any doubt as to whether it has occurred or by whom it was launched.”200

Because of the nature of the Internet, both of these issues are, in the context of the Internet, uncertain. Can a cyberattack be an “armed attack” if it only causes economic damage, or must it do physical damage?201 And if a cyberattack is launched against a state by foreign non-state actors, how can a state attribute the attack to state in which those actors reside?202

---

201 For a more detailed discussion of this question, see generally *ibid* at 76-95.
202 There are no decisions directly on this point. The two governing decisions on attribution with respect to non-state actors from international courts are the *Tadić* and *Nicaragua* decisions, which do not concern cyberwarfare and are of limited application. Both stand for the proposition that in order to attribute an attack carried out by non-state actors to the host state, the host state must exert some sort of control over the activities of the non-state actors, although they differ in their definition of control. See *Prosecutor v. Tadić*, IT-94-1-A, Judgment (15 July 1999) International Criminal Tribunal for the former Yugoslavia, Appeals Chamber; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States)*, [1986] ICJ Rep 14. The US Department of Defence takes the view that the United States is entitled to military intervention where the originating state is effectively incapable of controlling the conduct in question: United States Department of Defence, "An Assessment of International Legal Issues in Information Operations," (May 1999) online: Department of Defence <http://www.au.af.mil/au/awc/awegate/dod-io-legal/dod-io-legal.pdf> at 21-22. Some commentators suggest that IHL is moving in the direction of allowing for the attribution of state responsibility where states simply fail to act after their territory has been used to violate another state's rights, or after it has become clear that people within their territory intend to do so. See Vincent-Joel Proulx, "Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks?" (2005) 23 BJIL 615 at 625-646; Matthew J Sklerov, "Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent" (2009) 201 Mil L Rev 1 at 46.
largely anonymous nature of the Internet, and the ability to mask the geographical origin of an
attack, attribution becomes even more problematic.\textsuperscript{203} And even if one could attribute
the cyberattack to a given state, would it be permissible to physically strike at those non-state actors
or the civilian infrastructure used to carry out the attacks?\textsuperscript{204}

These questions remain formally unresolved, and the academic debate continues. Therefore,
despite the considerable challenges to IHL and LOAC raised by the Internet and cyberwarfare,
there has been minimal legal adaptation. The challenges and the academic response do, however,
suggest that the Internet has effectively a new front or battlefield that can be exploited in
wartime, and that it may have put considerable military power into the hands of non-state actors.

d. Contract and Commerce

The effect of the Internet on commerce and laws relating to contract has been quite extensive,
although most legal adaptations in these areas have been largely technical and prosaic, and
typically take the view of the Internet as simply another medium through which commerce and
contract can be transacted. For example, Canadian provincial electronic commerce statutes, such
as Ontario’s \textit{Electronic Commerce Act},\textsuperscript{205} primarily concern ensuring that electronic contracts
are enforceable and that electronic signatures can be used. They focus on the functional
 equivalency between electronic transactions and those that occur in the physical world. In other
words, many legal responses within this area of law are simply clarifications that existing
contract and commercial law applies to online and digital transactions.

The number of legal responses to Internet commerce, which are often made through discrete
amendments affecting particular issues, are too many to fully review here. Some other legal
responses include consumer protection legislation governing consumer contracts executed on the

\textsuperscript{203} For example, the Stuxnet virus used to attack Iranian nuclear enrichment facilities was only identified as likely
originating with the US and Israeli governments two years after the attack occurred. See \textit{supra} note 34.

\textsuperscript{204} Proportionality requires that the potential damage or injury to non-military targets caused by a retaliatory strike
be proportionate to the military importance of the target, and to the harm committed by the initial attack. Gary Solis, \textit{The Law of Armed Conflict}, (Cambridge: Cambridge University Press, 2010) at 272-275. For a more complete
discussion of retaliatory attacks on civilian infrastructure and non-state actors, see Eric Talbot Jensen, “Unexpected
Intl L Rev 1145; \textit{Sklerov, supra} note 202; Dinniss, \textit{supra} note 202 at 139-219.

\textsuperscript{205} \textit{Electronic Commerce Act}, 2000, SO 2000, c 17. Some similar acts in other provinces include \textit{Electronic
Transactions Act}, SA 2001, c E-5.5 (for Alberta); \textit{The Electronic Commerce and Information Act}, CCSM c E55 (for
Manitoba); \textit{Electronic Transactions Act}, SBC 2001, c 10 (for British Columbia).
the treatment of electronically stored and transferred funds, responses to cryptocurrencies like Bitcoin, and Internet advertising regulations. Some areas affected by the Internet that also may relate to commerce include privacy law, virtual property, and domain names and trade-mark law, but these are addressed elsewhere in this thesis.

The very briefly surveyed areas above primarily address new methods of committing harms created by the Internet and serving to enable electronic commerce by ensuring the enforceability of Internet agreements and the ability to transfer and use electronic funds and banking services. By and large, these legal adaptation represent an external view of the Internet by focusing on the actual commercial and contractual effects of online activity. They do not generally see the Internet as a separate place, but largely as a new mechanism to store and exchange funds and documents. While cryptocurrencies like Bitcoin may ultimately raise distinctive challenges for the law that are different in kind from other challenges to come before, little legal adaptation has yet occurred.

e. Copyright

Copyright law has undergone substantial changes in response to the Internet. Indeed, in both Canada and the United States, large legislative enactments have attempted to directly address the new challenges posed by the Internet on existing copyright law. It’s no great wonder why the Internet should induce such significant change. Copyright law, in the English tradition, was created as a response to the technology of the printing press, which had formed a new industry and thereby altered the distribution of wealth in society. Copyright law, at least in systems that follow the English tradition, has always been an attempt to balance the economic interests of the authors and distributors of creative works with the interest of the public

---

207 See e.g. Electronic Fund Transfer Act, Pub L No 95-630, 92 Stat 3728 (Federal US legislation).
211 See generally Morris, Jr, supra note 21 at 228.
Copyright law attempts to do this by providing copyright owners limited, exclusive, and alienable rights to control the copying, adaptation, translation, distribution and other uses of copyright-protected works.\(^\text{213}\)

As a legal regime fundamentally premised on a balance, this balance can become upset whenever a new technology changes the incentives and costs of production, distribution, or infringement. The Internet has done all of these things,\(^\text{214}\) and more. Indeed, the Internet has challenged the fundamental assumptions that underlie the notion of copyright: that controlling the copying of a work will control access and distribution.\(^\text{215}\) In this sense, the Internet has altered the underlying facts justifying the law (the fourth category from Chapter 1). While the changes to copyright have been many, the fundamental structure of copyright remains the same.

The challenges raised by the Internet and the associated legal adaptations are, again, too numerous to review in detail here, but some generalizations are possible when looking at the narrow example of Canadian copyright law.

The first generalization, mentioned earlier, is that the Internet has challenged a core assumption of copyright: that giving the author the right to control copying of her works will limit the ability of consumers to obtain access to those works. In a pre-Internet era, this assumption made sense, as obtaining a copy was generally the only way one could access and experience a work outside of public performances, or, in some cases, broadcasts. With the Internet, however, obtaining access to a work no longer required the creation of any kind of permanent copy, and it became less clear whether each individual case of access also constituted a “copy.” Indeed, due to the transient nature of works accessed through the Internet, and the number of “copies” made for purely technical purposes when transmitting data across the Internet, it became very unclear what the limits of a “copy” were.\(^\text{216}\) In Canada, these issues have been, at least in part, legislatively

\(^{212}\) See Landes & Posner, supra note 143 at 325 (“Copyright protection […] trades off the costs of limiting access to a work against the benefits of providing incentives to create the work in the first place” at 326).

\(^{213}\) Copyright Act, RSC 1985, c C-42, s 3(1).


\(^{216}\) See e.g. MAI Systems Corp v Peak Computer, Inc, supra note 138 (finding that a temporary copy put into RAM was a copy requiring authorization of the rights-holder).
addressed.\textsuperscript{217} Liability for the creation of copies for purely technical reasons has been limited,\textsuperscript{218} and a number of provisions have addressed the discrepancy between accessing a work and copying a work with respect to end users. These include a number of provisions that expand the ability of users to legally make copies of works, such as for back-up purposes or time-shifting,\textsuperscript{219} as well as a number that provide further access controls for rights-holders. These new access controls include granting rights-holders the exclusive right to make a work available through telecommunication in “a way that allows a member of the public to have access to it from a place and at a time and individually chosen by that member of the public”.\textsuperscript{220} Another major access-control measure was giving rights-holders legal recourse for the unauthorized circumvention of technological protection measures.\textsuperscript{221} Taken together, these legal adaptations signal a slow movement away from viewing the copy as the basis of copyright, but rather the control of access to works by users.

A second generalization is that the amendments to the Copyright Act in response to the Internet have altered the balance between copyright and freedom of expression, in many cases in favour of freedom of expression.\textsuperscript{222} While these amendments have also created implicit limitations on the use of works for expressive purposes by granting rights-holders additional control, such as enacting legal liability for the circumvention of technological protection measures, a number of provisions have also promoted the use of copyrighted works for expression. First and foremost is the considerable expansion of the explicitly recognized fair dealing exceptions to copyright infringement. The expansion of fair dealing in the Copyright Modernization Act includes fair dealing for the purposes of parody, satire, and education.\textsuperscript{223} The Supreme Court of Canada had, prior to these expansions, generally called the fair dealing exceptions “user rights” rather than

\textsuperscript{217} This legislation came in the form of the Copyright Modernization Act. Copyright Modernization Act, supra note 63.
\textsuperscript{218} Copyright Act, supra note 213, s 30.71.
\textsuperscript{219} Ibid, ss 29.23, 29.24.
\textsuperscript{220} Ibid, s 2.4(1.1). It might be argued that this isn’t an “access” control, but rather a subset of the public performance right. That may be true, however, the view presented here is that copyright was always implicitly about access control, and thus the public performance right was always a special type of access control.
\textsuperscript{221} Ibid, s 41.1. Technological protection measures refers to “any effective technology, device or component that […] controls access to a work.” Ibid, s 41. These measures are often referred to as digital rights management or DRM.
\textsuperscript{222} For a history of the balance between copyright and freedom of expression in the English tradition, see Pamela Samuelson, “Copyright and Freedom of Expression in Historical Perspective” (2003) 10 J Intell Prop L 319.
\textsuperscript{223} Copyright Act, supra note 213, s 29.
defences to infringement, and stated that they be interpreted liberally in order not to unduly burden the rights of users. The broadening of the fair use exceptions is therefore a broad expansion of the ability of users to use copyrighted works for expressive purposes. There is debate about whether the explicit inclusion of these categories of fair dealing is an expansion or merely a recognition of existing law. However, at least one Federal Court case had previously held that the Copyright Act did not allow for fair dealing for the purposes of parody, and many commentators had assumed that the categories were closed to those enumerated in the Act. Thus, the addition of parody, satire and education to the fair dealing provisions of the Copyright Act does appear to be, at least from a perspective of copyright users looking for certainty, an expansion.

The act also contained a notable new exception to infringement in the form of protection from liability for non-commercial user generated content. Commonly known as the “mash-up exception” or “YouTube exception,” the exception allows users to include copyrighted material into new works such as mash-up songs or home-videos, and share those works, so long as the use is not for commercial purposes, the copyrighted work was legally acquired, the source is named if reasonable in the circumstances, and the new work doesn’t negatively impact the market for the original. This exception, which was expressly created in contemplation of the new online ecosystem for user-generated content, is a fairly large shift in the balance between freedom of expression and copyright in favour of the former. Indeed, it has been suggested that it might go beyond the limits imposed by international copyright treaties.

225 Copyright Act, supra note 213, s 51.
228 See Katz, supra note 226 at 95 (additionally listing a number of major contemporary sources making this claim in footnote 10).
229 Copyright Act, supra note 213, s 29.21.
230 See e.g. Marian Hebb, “UGC and Fan Fiction: Rethinking Section 29.21” (2014) 26 IPJ 237 at 238.
231 Copyright Act, supra note 213, s 29.21.
232 See Hebb, supra note 230 at 238.
233 Ibid.
The non-commercial user generated content exception also implicitly recognizes the challenge raised by the Internet to another core assumption of copyright: that the promise of economic returns are necessary to spur the creation of new works. However, a number of scholars have, especially recently, questioned this assumption, and the empirical evidence strongly suggests that in the modern Internet ecosystem, the creation of new works remains strong even in the absence of meaningful financial returns to creators. The non-commercial user generated content exception represents an inherent recognition of this fact by virtue of expressly protecting the creation and dissemination of works for which the author can expect no possibility of financial remuneration (even if it requires ensuring that the market for any works incorporated into that work remains unaffected). It also serves to recognize the creativity, scope, and importance of user-generated content on the Internet, suggesting that the Internet has become an important medium not only for the dissemination of more traditional works, but also for users to interact with existing works in creative ways that result in entirely new works. Indeed, it may be a recognition of Internet culture as promoting a largely free, or sharing-based, economy.

f. Privacy

Privacy, Justice Binnie of the Supreme Court of Canada has said, is a “protean concept.” That is, privacy is a concept capable of taking on a number of different forms, and protecting what may be different interests. For example, Alan Westin, writing in response to the technological changes of the 1950s and 60s, identified four primary states of privacy, which might also be termed privacy interests: solitude, intimacy, anonymity and reserve. It’s quite possible that the Internet has affected all four of these interests, and in different ways.

---

234 For a more detailed explanation of this assumption, see Landes & Posner, supra note 143.
237 See Lessig, “Creative Commons”, supra note 214.
Perhaps the most remarkable impact of the Internet upon privacy is the ability for the Internet to track its users and compile records, profiles and databases of those users. As the Ontario Court of Appeal noted:

[| routinely kept electronic databases render our most personal financial information vulnerable. Sensitive information as to our health is similarly available, as are records of the books we have borrowed or bought, the movies we have rented or downloaded, where we have shopped, where we have travelled and the nature of our communications by cellphone, e-mail or text message.240 |

The collection and storage of personal information enabled by the Internet, coupled with the ability to create profiles of users based upon the aggregation of otherwise discrete pieces of information, has become a critical privacy risk. It is also the most readily apparent effect of the Internet, given that western societies tend to focus on the right to privacy as the control of information about oneself.241 Because of the clear privacy implications related to the collection, use and disclosure of personal information posed by the Internet, the majority of legal adaptations to the Internet with respect to privacy, at least in Canada, have concerned informational privacy and information control.

The primary legal response to informational privacy concerns raised by the Internet is the Personal Information Protection and Electronic Documents Act (PIPEDA). This statute, which regulates the private sector, operates throughout most of Canada, except in those provinces where provincial legislation has been declared “substantially similar.”242 While other legislation, such as the Privacy Act,243 concerns personal information held by governments, as PIPEDA

---

240 Jones v Tsige, supra note 77 at para 67.
241 “Introduction” in Identity Trail, supra note 14 at xxvii.
242 Personal Information Protection and Electronic Documents Act, SC 2000, c 5, s 26(2)(b) [PIPEDA]. At the time of this writing, only British Columbia, Alberta, and Quebec have substantially similar legislation that applies across the private sector, while Ontario, New Brunswick, and Newfoundland and Labrador have substantially similar legislation with respect only to personal health information: Organizations in the Province of Alberta Exemption Order, SOR/2004-219; Organizations in the Province of British Columbia Exemption Order, SOR/2004-220; Organizations in the Province of Quebec Exemption Order, SOR/2003-374; Health Information Custodians in the Province of Ontario Exemption Order, SOR/2005-399; Personal Health Information Custodians in New Brunswick Exemption Order, SOR/2011-265; Personal Health Information Custodians in Newfoundland and Labrador Exemption Order, SI/2012-72.
243 Privacy Act, RSC 1985, c P-21.
focuses on the private sector, it is of primary importance in regulating the bulk of the collection and use of personal information online.

PIPEDA is an express response to the Internet, designed to “promote electronic commerce by protecting personal information.”244 “Personal information,” for the purposes of PIPEDA, is “information about an identifiable individual,”245 meaning that the information in question must be capable of being tied to a specific identifiable person, as opposed to anonymized data. PIPEDA limits the collection, use, and disclosure of personal information by private organizations to “purposes that a reasonable person would consider are appropriate in the circumstances.”246 In most cases, such collection, use, or disclosure requires the informed consent of the individual to whom the information relates in order to be reasonable in the circumstances,247 although a large number of exceptions to this consent requirement exist.248

While the core concepts surrounding the protection of personal information in PIPEDA are relatively simple, the application of the statute to real world circumstances is not always clear. An example of this can be found in the position of the Privacy Commissioner of Canada with respect to online behavioural advertising (OBA).249 The Privacy Commissioner defines online behavioural advertising as “tracking consumers’ online activities, across sites and over time in order to deliver advertisements targeted to their inferred interests.”250 In order to do so, advertising networks collect numerous small bits of behavioural data and compile it into a profile with the intent to predict the user’s purchasing habits.251 While the information collected for the purposes of online behavioural advertising often does not contain directly identifying information, the Privacy Commissioner nonetheless found that all information collected for this purpose was “personal information” under PIPEDA.252 According the policy, the practice of online behavioural advertising involves the collection of information, which while not always

---

244 PIPEDA, supra note 242, preamble.
245 Ibid, s 2(1).
246 Ibid, s 5(3).
247 Ibid, Schedule 1, clause 4.3.
248 Ibid, s 7.
250 Ibid.
251 Ibid.
252 Ibid.
directly identifying the individual, should be considered personal information because it’s
*possible* that the information could be used to identify the individual, and because the
information may be used to serve highly personalized ads.\(^{253}\) However, despite finding that OBA
involved the collection and use of personal information of Internet users, the Privacy
Commissioner found that OBA could serve useful purposes, and thus could be reasonable in the
circumstances with appropriate disclosures and opt-out mechanisms.\(^{254}\) As this example
demonstrates, it is not always clear what sorts of uses of personal information might be
reasonably appropriate in the circumstances, nor what might qualify as personal information.
PIPEDA’s ability to protect sensitive information from collection and use is, therefore, less clear
to Internet users than it might be, and there are legitimate concerns that it strikes a balance
between business interests and consumer interests largely in the former’s favour.\(^{255}\)

Another limitation of PIPEDA is that it applies only to “organizations,” and can thus leave
victims of breaches of privacy without recourse where an individual was responsible for the
collection, use or disclosure of the personal information in question. In Ontario, the Ontario
Court of Appeal partially addressed this gap through the recognition of a tort of intrusion upon
seclusion.\(^{256}\) The tort, which is based largely upon a tort identified in the American Restatement
of Torts,\(^{257}\) consists of the following elements:

first, that the defendant's conduct must be intentional [or] reckless; second,
that the defendant must have invaded, without lawful justification, the
plaintiff's private affairs or concerns; and third, that a reasonable person
would regard the invasion as highly offensive causing distress, humiliation
or anguish.\(^{258}\)

The tort is clearly very broad and contemplates a large swath of possible conduct that is
unrelated to the Internet, or any technology. Regardless, both the facts of the case—which
concerned a bank employee accessing an individual’s bank records without lawful reason or

\(^{253}\) *Ibid.*

\(^{254}\) *Ibid.*

\(^{255}\) See e.g. Office of the Privacy Commissioner of Canada, “The Case for Reforming the *Personal Information
Protection and Electronic Documents Act*” (May 2013) online:
<https://www.priv.gc.ca/parl/2013/pipeda_r_201305_e.asp>.

\(^{256}\) *Jones v Tsige*, *supra* note 77.

\(^{257}\) *Ibid* at paras 18-19, 55.

\(^{258}\) *Ibid* at para 71.
authorization\textsuperscript{259}— and the express statements of the Court, indicated that the Internet was a motivating force behind the creation of the law due to the increased ability of individuals and organizations to intrude into someone’s private affairs using the technology.\textsuperscript{260} Thus the tort served as a legal adaptation to address, at least in part, an increased capacity for privacy intrusions on the Internet.

One other major recent judicial response to the Internet is the recognition of anonymity as a contextual right protected under section 8 of the \textit{Canadian Charter of Rights and Freedoms}.\textsuperscript{261} Unsurprisingly, the anonymity interest was recognized in a case concerning Internet activities (in this case, child pornography). The Court held that that the defendant’s privacy interests were engaged when the police obtained his subscriber information from the defendant’s Internet service provider without judicial authorization. Justice Cromwell, writing for a unanimous Court, noted that the privacy interest in anonymity arises, in part, from the fact that it allows individuals to express ideas, especially online, without being identified as the author.\textsuperscript{262} In his reasons, Justice Cromwell endorsed the view of Justice Doherty of the Ontario Court of Appeal in \textit{R v. Ward} that the Internet and anonymity are closely related.\textsuperscript{263}

\begin{quote}
[Justice Doherty] concluded that some degree of anonymity is a feature of much Internet activity and that, “[d]epending on the totality of the circumstances, […] anonymity may enjoy constitutional protection under s. 8”. […] I agree.\textsuperscript{264}
\end{quote}

That the anonymity interest appears to be particularly engaged in the online context has been slowly gaining recognition over the last half-dozen years. In \textit{Warman v Wilkins-Fournier}, the Ontario Divisional Court noted that there is “an implicit understanding of citizens that, to some degree at least, their identities will be protected when they use the Internet anonymously.”\textsuperscript{265}

\begin{itemize}
\item \textsuperscript{259} \textit{Ibid} at paras 2-5.
\item \textsuperscript{260} \textit{Ibid} at para 67.
\item \textsuperscript{261} \textit{R v Spencer, supra} note 140.
\item \textsuperscript{262} \textit{Ibid} at para 45.
\item \textsuperscript{263} \textit{R v Ward,} 2012 ONCA 660, 112 OR (3d) 321.
\item \textsuperscript{264} \textit{R v Spencer, supra} note 140 at para 48 (quoting \textit{R v Ward, ibid} at para 75).
\item \textsuperscript{265} \textit{Warman v Wilkins-Fournier,} 2010 ONSC 2126, 100 OR (3d) 648, 319 DLR (4th) 268 (Div Ct) at para 20.
\end{itemize}
The association between privacy and anonymity is not new to the Internet age, but the importance of anonymity, and the related pseudonymity, to privacy interests has begun to receive considerable legal attention in the online context.

As anonymity and privacy will be discussed at length in Part 3, below, I will leave a further discussion of these issues until that part. Nonetheless, this brief review indicates the Internet has changed the facts on which traditional notions of privacy are justified, engendered a number of new possible harms, and provided new means to inflict harms. The legal response to these issues has been wide-reaching, although, perhaps, very far from complete.

g. Defamation and Freedom of Expression

Defamation is a difficult issue to address in the online context. The nature of the Internet is one of often spontaneous but permanently (or at least temporarily) recorded speech that can be accessed from anywhere in the world. It thus both enables the publication of off-the-cuff statements that might not have been made in a more formal context, and gives such statements wide reach and longevity.267 The proper balance between the right to freedom of expression and the right to the protection of one’s reputation from defamatory speech is therefore more difficult to determine, as both the defamer and the defamed stand to lose much should it be poorly made.

Fortunately, by and large, existing defamation laws adequately address Internet defamation.268 Defamation on the Internet is not different in kind from defamation elsewhere, as the same interests are still at stake. However, there are some factors that suggest that there is at least some important differences of degree that have affected the traditional balance between freedom of expression and the protection of reputation, in some cases putting power into the hands of the defamer or the defamed.

The use anonymity and pseudonymity on the Internet is perhaps the most important difference between defamation on the Internet and defamation elsewhere. Anonymity or pseudonymity may

266 Ibid at para 42; Westin, supra note 239 at 31-32.
267 See Barrick Gold Corp v Lopehandia (2004), 71 OR (3d) 416, 239 DLR (4th) 577 (Ont CA) at paras 28-31.
268 See generally, ibid; Morris v Johnson, 2011 ONSC 3996, 107 OR (3d) 311; Warman v Wilkins-Fournier, supra note 265.
form a shield for defamers that makes them feel freer to openly make libellous statements without fear of reprisal or liability. This is understandable, as unmasking anonymous or pseudonymous posters can be difficult, or, in some cases, practically impossible where the poster has taken steps to hide their identity.269 Because of this, many academics have called for less protection for anonymity on the Internet, claiming that the Internet inherently puts too much power in the hands of the defamers and undermines the ability of individuals to defend their reputations.270

Following the widespread use of anonymity by defamers, courts have been faced with the challenge of deciding when it is appropriate to order a third party intermediary, such as an internet service provider or forum host, to disclose information concerning the identity of the defamer sufficient to bring an action.271 This naturally puts the interests in privacy, freedom of expression, and the protection of personal reputation in conflict. In both Canada and the United States, the general view is that such disclosure can only be ordered where all other reasonable mechanisms of contacting and determining the identity of the defamers has been attempted and that a prima facie defamation case has been made out.272

But these procedural mechanisms to reveal the identity of defamers have, in some ways, put an unexpected power in the hands of those who wish to silence others on the Internet. This can be done through what are sometimes called “strategic lawsuits against public participation,” or cyberSLAPPs.273 In a cyberSLAPP, litigants initiate defamation proceedings against anonymous online speakers in order to reveal their identities. In doing so, the litigant seeks to silence the impugned speech simply through the threat of revealing the identity of the alleged defamer, even if the litigant is unlikely to win a defamation suit.274

---

269 For the more tech-savvy Internet users, there are many methods of ensuring effectively total anonymity. See Andy Greenberg, “How to Anonymize Everything You Do Online,” Wired (17 June 2014), online: <https://www.wired.com/2014/06/be-anonymous-online/>.
271 See e.g. Warman v Wilkins-Fournier, supra note 265 (in Canada); Independent Newspapers, Inc v Brodie, 966 A (2d) 432 (MD 2009) (in the US).
272 Ibid.
273 Richards, supra note 6 at 523-524.
274 Ibid.
This strange and counterintuitive placement of power in the hands of both defamers and the defamed, and the risks of either side abusing the power, have required careful balancing. Indeed, it can be said that the Internet has altered the facts justifying existing law with respect to defamation and freedom of expression as well. Because of the perceived harms of this invasion of privacy and the potential chilling effects of these lawsuits on freedom of speech, many US courts have expanded protections around anonymity in defamation cases. These protections generally serve to increase safeguards against revealing the identity of anonymous users where the defamation suit has little merit. In particular, a number of courts have held that before a disclosure order can be made, not only must the plaintiff demonstrate a *prima facie* defamation case, but the court must balance the strength of that *prima facie* defamation case against the First Amendment rights of the alleged defamer. Not all US courts have embraced this balancing, however, in some cases finding that demonstrating a *prima facie* case is sufficient. As Professor Lidsky has noted, the approach to anonymous defamation remains piecemeal, “developing case-by-case and court-by-court.”

In Canada, these cases are much rarer, but defamation cases both prior to and following the Supreme Court of Canada’s decision in *R v. Spencer* have suggested that privacy and freedom of expression interests must be considered before a court can order the identities of anonymous alleged defamers to be revealed. Indeed, in *Warman v. Wilkins Fournier*, the Ontario Divisional Court stated that disclosure of the identities of anonymous alleged defamers online risked a “chilling effect on freedom of expression” and suggested that “a more robust standard is required [than that of *BMG v. Doe*]” in considering whether to order disclosure. This “more robust standard,” like that established by most US courts, requires a *prima facie* protection.

---


276 See e.g. *Independent Newspapers, Inc v Brodie*, supra note 271 at 457; *Dendrite International Inc v Doe*, No 3, 775 A (2d) 756 (NJ Super Ct App Div 2001).

277 See e.g. *Doe No 1 v Cahill*, 884 A (2d) 451 (Del Supreme Ct 2005).

278 Lidsky, *supra* note 275 at 1385.

279 See e.g. *Warman v Wilkins-Fournier*, *supra* note 265; *Morris v Johnson*, *supra* note 268; *King v Power*, 2015 CanLII 11200 (NL SCTD).

280 *Warman v Wilkins-Fournier*, *supra* note 265 at para 42.

281 *Ibid*, referring to *BMG Canada Inc v Doe*, 2005 FCA 193, [2005] 4 FCR 81, 252 DLR (4th) 342 (in which the test was established for ordering the disclosure by a third-party ISP of subscriber information necessary to bring an action for copyright infringement).
defamation case to be demonstrated by the plaintiff before the disclosure order can be made282: a requirement absent in the copyright context of BMG v Doe. However, unlike the US, there is generally no requirement that the freedom of expression interests of the defamer be balanced against the strength of the prima facie case demonstrated by the plaintiff.

Regardless, while there is no clear judicial consensus or overarching legislative response to the issues posed by defamation online, the response by the common law still underscores the unique nature of defamation online. As the Ontario Court of Appeal has said: “is there something about defamation on the Internet […] that distinguishes it, for purposes of damages, from defamation in another medium? My response to that question is "Yes."”283 The response discloses a general shift in the normative balance between the protection of reputation and freedom of expression, and underscores the unique nature and importance of anonymous speech on the Internet.

h. Electronic Communications Spam

The Internet has enabled many new means of instantaneous and inexpensive communication that allow people to connect around the world. At the same time, however, it’s also enabled advertisers, scammers, and others looking to contact a broad audience a medium through which they can cheaply send unsolicited messages to unwitting recipients. These messages, which are often called “spam,” can be made through any communication platform that allows the sending of discrete messages to individual electronic addresses. Email spam, in particular, has long been a major concern of Internet users, causing reactions ranging from mere annoyance to vehement rage.284 There are obvious harms to spam. It is annoying, certainly, and there have been reports suggesting that it creates economic losses due to the time expenditure in deleting or otherwise dealing with spam messages as well as the extra server capacity required to handle it.285 It may even be that, without efficacious spam filtering technologies, email may be rendered largely unusable.286 Spam has also been described as “viscerally offensive to the general public,”287 and

282 Ibid at para 42.
283 Barrick Gold Corp v Lopehandia, supra note 267 at para 28.
286 Ibid at 88.
287 Slane, supra note 284 at 263, quoting KK Campbell, "Web Advertising In Search of a Model," Toronto Star (10 April 1997) at G5.
“an egregious intrusion of online space, and [...] a pernicious evil to Internet usage,” suggesting that spam is also a form of personal intrusion. While the harm of spam will be discussed later in this chapter, it suffices to say for now that it is another way through which the Internet has given rise to new harms, or at least new methods of inflicting a harm.

The law has not been blind to the harm. Some American court cases considered the application of the tort of trespass to chattels, discussed in Part 2(a) above, finding that the tort could apply, even if plaintiffs were not always successful. However, the use of the tort to address email spam was criticized due to its limited ability to address the harm and the courts’ alleged conflation of the torts of trespass to chattels and trespass to property. At least one commentator noted that nuisance law might be the proper method by which to address spam. Unfortunately, the common law has not conclusively addressed the issue of email spam.

To the extent the issue has been addressed with any finality, however, it has been addressed through legislation. Some American states, such as California, were early adopters of anti-spam legislation with respect to email. California’s law was based on a similar provision that previously addressed similar unsolicited messages sent through fax, and it only set out content requirements, including a necessary unsubscribe (opt-out) mechanism, rather than prohibiting it outright. It wouldn’t be until 2003 that the US addressed spam federally through legislation commonly known as CAN-SPAM, a backronym for Controlling the Assault of Non-Solicited Pornography and Marketing. The statute regulates “commercial electronic mail messages,” which are defined as “any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content

---

288 Hunter, supra note 147 at 478.
289 See e.g. CompuServe, Inc v Cyber Promotions, Inc, 962 F Supp 1015 (SD Ohio 1997) (finding liability of a spammer to an Internet service provider due to interference with the operation of their systems); America Online, Inc v IMS, 24 F Supp (2d) 548 (ED Va 1998) (also finding liability of a spammer to an Internet service provider due to interference with the operation of their systems); Intel Corp v Hamidi, supra note 144 (no liability for a spammer where the spam email did not meaningfully interfere with the plaintiff’s chattels, although the tort could apply).
291 Kam, supra note 27.
293 Ibid.
on an Internet website operated for a commercial purpose).” However, like the California law that preceded it, CAN-SPAM does not ban the practice of sending unsolicited commercial messages. Instead it includes a number of compliance requirements, such as the inclusion of an unsubscribe mechanism, the inclusion of proper ‘from’ and ‘subject’ lines, limitations on the use of harvested email addresses, and other technical restrictions.

Canada’s response to spam came much later on, but in the much more robust form of a 2010 statute commonly known as Canada’s Anti-Spam Law, or CASL. Like CAN-SPAM, it focuses its attention only on those email messages with a commercial purpose. However, unlike CAN-SPAM, CASL prohibits the sending of unsolicited electronic messages without obtaining a form of consent, either express or implied. The categories of implied consent are complex, but they do generally allow businesses to get in contact with existing customers, and for businesses to contact other businesses with whom they have a relationship. The manner by which express consent is obtained is also subject to a number of procedural and disclosure requirements. Failure to abide by these limitations can result in an administrative monetary penalty of up to $10,000,000 for organizations. While CASL’s stated purpose is largely to promote the confidence of businesses and consumers in the online marketplace, CASL is also clearly aimed at protecting consumers from the annoyance of spam, the intrusion into their personal space, and the possible dangers of malicious emails. Indeed, in 2017, a private right of action will come into force that will allow consumers to sue spammers directly, rather than rely upon the enforcement of public agencies.

---

296 15 US Code § 7704.
297 The statute is known as CASL because its actual name is rather long: An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act. See CASL, supra note 60.
298 Ibid, s 1(2).
299 Ibid, s 6.
300 Ibid, s 10(9).
301 Ibid, s 10(1).
302 Ibid, s 20(4).
303 Ibid, s 3.
305 CASL, supra note 60, ss 47-51.
The legal response to spam has been surprisingly extensive, with both courts and legislatures attempting to curtail its transmission. These responses, as well as the contempt with which spam appears to be held by the general public,\textsuperscript{306} indicate a strong societal perception of harm arising from its use. A more detailed explorations of the reasons for this perception will be addressed in the next part.

3. Finding a Common Theme

This review of legal responses to the Internet is certainly a cursory one, but it is nonetheless sufficient to identify some potential commonalities worth further investigation. As we’ve seen, legal responses are often predicated upon the perspective the decision-maker takes of the Internet.\textsuperscript{307} External views tend to view the Internet in a more literal and technical sense. This leads to adaptations focused on ensuring that the Internet works as a tool for communication and business transactions, while attempting to limit the possible harms that can arise from a ubiquitous and inexpensive data transfer mechanism.\textsuperscript{308} We see this kind of external view taken frequently with respect to ecommerce, copyright, defamation, and, sometimes, the criminal law. On the other hand, the internal view of the Internet sees it as a sort of place inhabited and explored by its users.\textsuperscript{309} This leads to legal responses that attempt to both regulate and enable the use of the Internet as a platform for self-expression, exploration, and ownership. These kinds of legal responses are sometimes seen within the areas of privacy, property and trespass, email spam, and to a more limited extent, criminal law and copyright.

It is these latter areas—in which the legal responses largely take the internal view—that are most interesting. They are interesting because they are, in a manner, different in kind from the technical and instrumentalist responses one would expect to a technology. This internal view appears to be increasingly common in judicial decisions, perhaps as experience with the Internet grows amongst the judiciary. This can be seen in the way the Supreme Court of Canada has described the Internet over the past decade and a half. For example, in 2004, the Supreme Court of Canada described the Internet in mundane terms as “a huge communications facility which

\textsuperscript{306} Slane, supra note 284 at 260-263.
\textsuperscript{307} See Bellia et al, supra note 146 at 32.
\textsuperscript{308} Ibid.
\textsuperscript{309} Ibid.
consists of a worldwide network of computer networks deployed to communicate information.”³¹⁰ Whereas, twelve years later, in a very recent decision, the Supreme Court described the Internet simply as “an indispensable tool of modern life and an avenue of democratic participation”.³¹¹

The external view, therefore looks at what the technology actually is, and what it can accomplish in a consequentialist sense. This view is unlikely to see the Internet as a realm or landscape that one can explore, or even claim a part of, except in the most metaphorical sense. And while the Internet-as-a-place notion may also be a metaphor, it often doesn’t feel like a metaphor at all. Indeed, the internal view of the Internet sees the Internet-as-place as more than a metaphor; it sees it as an apt description of the experience of using it. When the law recreates the law of trespass in the virtual world,³¹² or when it treats online anonymity in a manner similar to anonymity in a public place,³¹³ it’s clear that the courts are moving beyond metaphor, too.³¹⁴

The experiential aspect is thus critical to understanding the internal view of the Internet. While the modern Internet is still very far from a Matrix-esque virtual reality, it nonetheless creates a sense of place and of community. Understanding that the law often takes an internal view of the internet is a first step to narrowing our focus towards more important commonalities between legal adaptations. It demonstrates the important conclusion that the engagement of users with the Internet is often experiential and personal. One cannot understand many of the issues raised by the Internet, or the legal responses to the Internet, solely by taking an external and instrumentalist approach. That view cannot contemplate the lived experience of Internet users, and therefore cannot address the interests of those users nor the harms they might endure as part of that experience.

Yet the law, it seems, has been sensitive to these issues. Legal responses in the area of privacy, for example, have necessarily addressed the experiential aspects of Internet use. The protection of anonymity and the limitations on the collection, use and disclosure of personal information

---

³¹¹ R v KRJ, 2016 SCC 31.
³¹² See Hunter, supra note 147 at 486.
³¹³ R v Spencer, supra note 140 at paras 44-45.
³¹⁴ See Chapter 2, Part 2(a), supra.
serves to ensure that users can communicate, form communities, or simply find the content they desire without being tracked or identified. These privacy protections may appear to be simple responses to the increased capacity for third parties to collect personal information, but anonymity and privacy are a large part of what enables users to use the Internet in the ways that they do.\footnote{Kerr, Steeves & Lucock, supra note 14 at xxiii.} The architecture of the Internet may facilitate anonymity, but the architecture can be altered, and no one architecture is necessary to the existence of the Internet.\footnote{See Lawrence Lessig, “The Architecture of Privacy,” (1999) 1 Van J Ent L & Prac 56.} That the law has stepped in to protect, at least to some degree, the existing anonymizing architecture of the Internet is responsive to the internal view of the Internet insofar as it protects the very foundations of the existing Internet experience. Using the Internet without any anonymity or privacy, one can imagine, would be very different experience than using the existing Internet.

Privacy is not the only area in which the law has been sensitive to the lived experience of Internet users. Spam messaging, too, has been widely legislatively addressed for reasons that appear to go well beyond protecting the technological infrastructure of the Internet. Indeed, there are reasons to believe that one of the harms being legislatively addressed is one more closely related to an invasion of private or personal space.\footnote{See Slane, supra note 28.} Calls to deal with spam as a form of nuisance are illustrative of this harm,\footnote{See e.g. Adam Mossoff, “Spam—Oy, What a Nuisance!” (2004) 19:2 BTLJ 625; Kam, supra note 27.} as is the initial attempt to deal with spam as a form of trespass to chattels.\footnote{See e.g. Intel Corp v Hamidi, supra note 144; CompuServe, Inc v Cyber Promotions, supra note 289.} Spam may be an intrusion into, and interference with, the use of the Internet in a manner similar to the intrusion into the home created by other nuisances or trespasses.

The shift in the balance between copyright and freedom of expression, as demonstrated through the new fair dealing rights and the non-commercial user generated content exception to infringement,\footnote{Copyright Act, supra note 213, s 29-29.21.} is also responsive to the new ways in which users express themselves through the Internet. The express affirmation of these rights inherently recognizes that the Internet is not simply a tool through which the marginal cost of reproduction approaches zero, as the content industries may see it,\footnote{See e.g. Jessica Litman, “Real Copyright Reform” (2010) 96 Iowa L Rev 1 (generally discussing the view of content industries with respect to copyright).} but also one that provides a medium and an audience for transformative capabilities.
uses of existing content. While other adaptations may serve to grant copyright holders increased power over their works, the expansion of the exceptions to infringement at least acknowledges the importance of largely user-driven content services like YouTube, Instagram, SoundCloud and many others. These services have created the ecosystem and community in which the free exchange of user generated content can be made, without requiring users to incur the significant creation and distribution fees that would have been necessary in the pre-Internet era. This has led to an explosion of content for which no compensation is sought, and a culture of sharing and free exchange. It is this culture, and the value placed in it, that the law has, in my view, responded to.

Similarly, the balancing of freedom of expression and the protection of reputation in anonymous defamation proceedings in the online context is also illustrative of a regard for the culture of the Internet and the experience of its users. The near universal acceptance by the courts of a requirement to consider freedom of expression interests before ordering the disclosure of the identifying information of an anonymous defamer reflects the importance of online anonymity to Internet speech. While anonymity has been historically protected through freedom of expression, issues concerning anonymity and disclosure were much rarer before the Internet. The wide use of anonymity on the Internet has created a cultural shift with respect to individuals’ expectations of privacy in their communications and the way in which individuals interact with each other. While nothing in the technology of the Internet makes anonymous communication necessary or inevitable, the rise of an anonymous culture has been recognized and protected, to at least some degree, by the law. A respect for the importance of freedom of expression on the Internet is also reflected in the holding of Crookes v Newton that the posting of a hyperlink to defamatory content is not itself publication of the defamatory statement. A holding to the contrary would undoubtedly chill speech and prevent the flourishing of expression online.

A theme can thus be discerned: the law has been responsive to the cultural norms that have been created in the online context. These norms are by no means a necessary result of the underlying

322 For example, the legal prohibition on the circumvention of technological protection measures. Copyright Act, supra note 213, s 41-41.1.
324 See Part 2(g), supra.
325 Richards, supra note 6 at 534-535.
326 Crookes v Newton, supra note 51.
technology of the Internet, but are instead the result of complex social constructions arising from
the new ways of human interaction and exploration facilitated by the Internet. Indeed, one of the
most prevalent commonalities of these adaptations, at least with respect to those that take an
internal view of the Internet, is that they serve to protect the personhood interests of Internet
users. As will be discussed in greater detail in the next Chapter, anonymity, privacy, freedom of
expression, and protection from trespass and intrusion are all fundamental to the autonomy and
wellbeing of individuals. They are personhood interests, because they are constitutive of the
personhood of people. We are not ourselves without them; our self-definition is largely
predicated upon them.

It may be tempting to say the legal adaptations that have been made with respect to these
interests in the Internet context are merely attempts at maintaining the status quo in the face of a
destabilizing technology. That is, we might say that the law has simply attempted to ensure that
individuals enjoy the same level of freedom from harms and protections for their interests as they
enjoyed prior to the Internet. This is certainly true in some respects. However, we must recognize
that the goal posts have shifted. The context has changed, and what it means to have freedom of
expression, anonymity, or privacy in the online context may be fundamentally different from
what it meant before that context existed. So while the law may reach for the same standard of
protection, that standard when applied to the Internet begins to look different because of the
cultural and experiential shift engendered by the technology. The harms and the interests are
both the same and new. I acknowledge that this may sound unnecessarily obtuse. An example
may be helpful.

Consider our privacy interests with respect to anonymity. This was one of the basic states of
privacy identified by Alan Westin in his seminal 1967 work Privacy and Freedom.\(^{327}\) There, he
described anonymity as the ability to “merge into the situational landscape” of public spaces.\(^{328}\)
He considered anonymity to be the ability to participate in the public arena without being subject
to extensive surveillance and tracking, largely because the individual does not wish to be held to
“the full rules of behaviour and role that would operate if he were known to those observing

\(^{327}\) Westin, supra note 239 at 31-32.
\(^{328}\) Ibid.
him.” We can undoubtedly relate to this desire. We often feel constrained by the social norms imposed on us by those who may identify us or recognize us. Sociologists have noted that complete strangers are, for this reason, often made privy to personal confessions that would not be made to family or close friends. In the Internet context, however, this anonymity interest expands enormously. While the core of the interest lies in not being held to the “rules of behaviour” that attach to an individual when identified, the Internet allows one to interact publicly while hiding even the core identity information that would be readily apparent in a face-to-face meeting, such as age, gender, or ethnicity. “On the Internet,” the cartoon goes, “no one knows you’re a dog.” The Internet thus facilitates anonymity to a deeper degree than the anonymity one might expect at, say, a public market. Online anonymity is, in a sense, complete, and therefore facilitates the creation and exploration of entirely new identities. Additionally, as the Internet allows rapid and simultaneous communication with a large number of people, an individual’s anonymized identity can also be presented to a wider audience than might be expected in real space. The whole world can be treated as the stranger in which one confides. Anonymity on the Internet thus runs both deeper and wider. While the same concerns that have always motivated protections for anonymity continue in the Internet context, continuing the same level of legal protection for Internet anonymity as given to real world anonymity both requires different methods and enables different kinds of conduct than those protections in the real world. We must be cognizant that even in protecting well recognized interests against recognized harms, we might, in an important sense, be doing something new.

Legal protections for well-established personhood interests, then, can morph in the Internet context, and the law appears to have been responsive to this. It is not necessarily that the basic personhood interests are different in the Internet context, but the way in which those interests manifest, and the ways in which they might be harmed, may be different. In my view, the legal adaptations discussed earlier in this Chapter lead to a sort of “digital rights” that are responsive to the way that personhood interests manifest online. The rest of this Chapter will further explore

---

329 Ibid.
332 See Gaia Bernstein, supra note 8.
the legal adaptations that disclose these “digital rights” and the personhood interests that motivate them.

The theme identified here might be seen as an optimistic one, in which the law has responded in a positive way to shield the rights of users and promote individual personhood. I am certainly not blind to the many problems and overreaches by both the government and business on the Internet. Further, within the legislative arena, overly broad and restrictive legal adaptations such as the previously discussed Computer Fraud and Abuse Act in the United States might be seen to undermine the argument made in this Chapter. However, in my view, at least with respect to the areas of law surveyed here, the law has largely changed to attempt to limit abuses by both the government and businesses online. In this, the argument in this thesis may suggest that the legal adaptation to the Internet has been, in some ways, more protective of individual rights than those who focus on the many problems of the intersection of law and the Internet may acknowledge. I also appreciate that, with respect to the existing state of affairs on the Internet, it may well be that the law hasn’t successfully kept up, and that personhood interests are thus undermined in practice even if the law attempts to protect them. However, this thesis is concerned with legal adaptation to technological change, and in my view the legal change with respect to privacy, freedom of expression, and email spam has shown a clear trend towards increasing protections for personhood. Thus, despite the pessimism with which it is common to address legal issues on the Internet, in my view, it remains important to recognize the legal trends that promote individual personhood so that they might be considered in future legal developments, even if the adaptations may only have had a minor practical effect to date.

Additionally, as discussed in Chapter 1, my objective is to establish a single substantive theory of legal adaptation to the Internet and demonstrate its utility in dealing with potential future legal challenges raised by it. It must be remembered that there may be many possible substantive theories of legal adaptation to a single technological change without any conflict between them. They might simply address different issues and different kinds of responses, and as I discussed in the first Chapter, it’s possible that some of these might conflict. However, my aim here is only to explore and develop one such substantive theory, which in this case, is an exploration of the expansion of personhood interests in the Internet context. I do not claim this to be the only
possible substantive theory, but it is the one that will be addressed here. The rest of this thesis is devoted to precisely this task.

4. Digital Interests and Internet Rights

So far in this Chapter, I have discussed a number of legal adaptations to the Internet, and found that one commonality among them is that they seek to respond to the unique ways personhood interests are implicated in the online context. Now I turn to a deeper analysis of the specific legal responses that address personhood interests in order to elucidate the particular ways that the law has addressed these interests, and what that says about how the interests manifest in the Internet context.

a. Anonymity, Privacy and Identity

I’ve already briefly discussed the ways in which the anonymity interest online differs from the anonymity interest in not being tracked or identified in real space, especially as it relates to the suppression, and in some cases, subversion of identity. However, the relationship between anonymity and identity is a complex one, especially in the Internet context. In my view, this relationship is central to understanding the special attention, and perhaps protection, granted by the courts to Internet anonymity.

And the courts have given special attention to Internet anonymity as a privacy interest. In Canada, the most authoritative protection for Internet anonymity came from the Supreme Court of Canada in the case of *R v. Spencer*. The case concerned a criminal prosecution for child pornography. The issue on appeal to the Supreme Court was whether the accused’s privacy rights under section 8 of the *Canadian Charter of Rights and Freedoms* were violated when the police obtained his subscriber information from the defendant’s Internet service provider without judicial authorization. Justice Cromwell, writing a unanimous judgment, held that anonymity may be a constitutionally-protected privacy right under section 8 in certain

---

333 *R v Spencer, supra* note 140.
335 *R v Spencer, supra* note 140 at para 48.
contexts. Despite the relatively careful terms used by the Justice Cromwell, the judgment has been widely hailed as a landmark privacy decision.

Justice Cromwell noted that the interest in anonymity arises, in part, from the fact that it allows individuals to express ideas online without being identified as the author. Indeed, a close reading of the decision suggests that the Internet context was critical to the protection of anonymity under section 8 right. Justice Cromwell stated that there “is also a third conception of informational privacy that is particularly important in the context of Internet usage. This is the understanding of privacy as anonymity.” He reiterates the point again later in the decision: “Recognizing that anonymity is one conception of informational privacy seems to me to be particularly important in the context of Internet usage.” In addressing the concern of an intervener, the Attorney General of Alberta, he also suggests that this protection for anonymity might not hold in real world situations. The Attorney General’s concern was that a privacy right to anonymity would prohibit police from obtaining witness statements where those statements might include core biographical information of the suspect. The Supreme Court stated that such a result does not follow, and whether a privacy interest could be said to exist in such a statement would depend on the totality of the circumstances. However, given the importance that the Supreme Court places on the ability of Internet subscriber information to tie an individual to their Internet activity, it’s hard to imagine a scenario in which an attempt by police to obtain Internet subscriber information would not engage a privacy right under section 8.

Indeed, Canadian courts have increasingly been recognizing an anonymity interest in online activity. In Warman v Wilkins-Fournier, the Ontario Divisional Court noted that there is “an

336 Ibid at paras 2-5.
338 R v Spencer, supra note 140 at para 45.
339 Ibid at para 41.
340 Ibid at para 45.
341 Ibid at para 67.
342 Ibid.
343 Ibid at paras 47-50.
implicit understanding of citizens that, to some degree at least, their identities will be protected when they use the Internet anonymously.” And the Supreme Court in *Spencer* referred to the Ontario Court of Appeal decision in *R v Ward* to assert that the anonymous nature of a large amount of Internet activity may give rise to constitutional protection. The *Spencer* decision is thus a logical extension of the growing recognition of the importance of anonymity. It will certainly be interesting to see if future decisions further entrench rights to anonymity, or begin to claw back against it in favour of plaintiffs. In either case, it’s clear that anonymity on the Internet has brought anonymity into the legal foreground and forced Canadian courts to reconsider what privacy rights consist of.

Canadian courts have not been the only ones to recognize the importance of Internet anonymity. In the United States, the courts have traditionally protected anonymity as an element of the First Amendment guarantee of freedom of speech. While it does not concern the Internet, the leading case on anonymity and speech in the United States is *McIntyre v. Ohio Elections Commission*. In that case, the Supreme Court of the United States held that an Ohio law that prohibited anonymous publication of any material that might influence an election was unconstitutional. The anonymous publication at issue was not only held to be protected by the First Amendment, but part of an “honorable tradition of advocacy and dissent.” This protection for anonymity under the First Amendment has led to increased protections for anonymity online. In *Dendrite International Inc v Doe, No 3*, the New Jersey Superior Court established the test for ordering a third party to release identifying information about anonymous defendants that is now used widely in defamation cases. The test requires that the plaintiff has attempted to contact the anonymous defendants, that plaintiff has identified the specific statements allegedly made by the anonymous defendants, that plaintiff has established a prima facie defamation case, and finally that the “court balance the defendant’s First Amendment right of anonymous speech against the strength of the prima facie case presented and the necessity for the disclosure of the anonymous defendant’s identity”. This final balancing step arises

346 US Const amend I.
348 Ibid at 357.
349 *Dendrite International Inc v Doe, No 3*, *supra* note 276.
350 Ibid at 141-142.
uniquely within the Internet context. While this test has not been followed in all jurisdictions, it has been followed widely enough\(^{351}\) to suggest that the courts are moving in the direction of increasing protections for online anonymity, at least where protected speech is involved.

The attempts of the court to address the question of the proper balancing of anonymity, freedom of expression, and the interest plaintiffs or the government may have in identifying defendants, may not be sufficient to declare anonymity a uniquely digital right. Indeed, anonymity has certainly been protected in the pre-Internet context, such as in Canadian privacy decisions,\(^ {352}\) American First Amendment jurisprudence,\(^ {353}\) and even in Canadian copyright law.\(^ {354}\) However, it appears that the importance, breadth and depth of the anonymity interest is quite different in the Internet context based upon the recent rise in interest in anonymity, and the apparent increase in protections granted by the courts. Therefore, while anonymity itself may not be a uniquely “digital right,” the interests that anonymity protects may be more deeply held by more individuals in the Internet context, and the more extensive manner in which anonymity has been addressed and protected on the Internet might lead us to call it a “digital right” separate from traditional anonymity rights. Why it might be that anonymity is special in the Internet context requires us to look more deeply at why anonymity matters online.

Unfortunately, the courts have had a great deal of difficulty identifying the interests that anonymity protects online, and therefore why anonymity is so important in the Internet context. Decisions with respect to anonymity on the Internet are replete with broad statements concerning the importance of anonymity, and stressing the significance of anonymity in the Internet context, but they rarely cohere meaningfully to identify why it is that anonymity has become so central to online privacy. For example, in \(R \text{ v Ward}\), the Ontario Court of Appeal was at pains to describe the importance of privacy, but did not offer a compelling reason for why such import attaches to it. Writing for the Court, Justice Doherty stated that “[t]he fundamental importance of personal privacy cannot be denied. Personal privacy is a prerequisite to individual liberty, security, self-fulfilment and autonomy.”\(^ {355}\) With respect to anonymity, he went on to write that “[p]ersonal

---

\(^{351}\) See generally Lidsky, *supra* note 275.

\(^{352}\) See e.g. \(R \text{ v Wise}\), [1992] 1 SCR 527.

\(^{353}\) See e.g. McIntyre v. Ohio Elections Commission, *supra* note 347.

\(^{354}\) The Canadian *Copyright Act* protects the right of an author to remain anonymous with respect to a work. *Copyright Act, supra* note 213, s 14.1(1).

\(^{355}\) \(R \text{ v Ward, supra} \) note 263 at para 61.
privacy protects an individual’s ability to function on a day-to-day basis within society while enjoying a degree of anonymity that is essential to the individual’s personal growth and the flourishing of an open and democratic society.”356 These are powerful statements, but it remains unclear how they apply to the Internet context, nor precisely how Internet anonymity promotes “personal growth and flourishing” or “security, self-fulfillment and autonomy.”

Even in *R v Spencer*, the Supreme Court fell short of articulating a strong rationale for the protection of anonymity, even while advancing its legal protections. In defending anonymity as an important interest, Justice Cromwell quoted the above-noted language of Justice Doherty in *R v Ward*, citing his “usual insight and clarity.”357 The Court added that “anonymous Internet activity engages a high level of informational privacy”358 and that “anonymity is an important safeguard for privacy interests online.”359 Why is this? The Court referred to a number of possible reasons. There was a suggestion that it follows from a need to allow the expression of ideas without being identified as their author.360 There was an assertion that online anonymity increases informational privacy by preventing third parties from compiling a pattern of online activity about an individual, such as for use in OBA.361 Finally, and most importantly, the court made reference to a passage from Alan Westin’s *Privacy and Freedom*, in which he introduces the idea of anonymity as one state of privacy that allows individuals to “act in public places but to preserve freedom from identification and surveillance.”362 The Ontario Court of Appeal in *R v Ward* referred to this same passage.363 Unfortunately, neither court went beyond Westin’s introduction to the idea of anonymity as a form of privacy to examine why anonymity is necessary to self-development, autonomy or human flourishing. The American courts have fared little better, focusing instead on the value of anonymity to protect the ability to speak freely without fear of recourse and as a “shield from the tyranny of the majority.”364 While this is

357 *R v Spencer, supra* note 140 at para 48.
358 *Ibid* at para 55.
359 *Ibid* at para 79.
360 *Ibid* at para 45.
361 *Ibid* at para 46.
363 *R v Ward, supra* note 263 at para 73.
364 See e.g. *McIntyre v. Ohio Elections Commission, supra* note 347 at 357.
undoubtedly a very important reason to protect anonymity, it does not fully describe the importance of anonymity as a privacy interest in the Internet context.

To fully understand why anonymity online is so important, we must understand why anonymity, and even privacy, is so important to “liberty, security, self-fulfilment and autonomy.”\textsuperscript{365} In \textit{Privacy and Freedom}, Alan Westin identifies four core interests that privacy seeks to protect. These are “personal autonomy, emotional release, self-evaluation, and limited and protected communication.”\textsuperscript{366} Only the first three of these is particularly relevant for our discussion of anonymity on the Internet.

Westin’s first core privacy interest, personal autonomy, is especially important with respect to anonymity online. Personal autonomy is, in Westin’s view, a necessary part of being a self-actualized individual person, free from manipulation or domination by others.\textsuperscript{367} Manipulation and domination, however, does not require physical coercion. One method of coercing a person is by gaining access to information and secrets of the target individual that that individual does not desire to be publicly known, or known to certain other individuals. The examples of this are obvious in cases of blackmail or extortion. But the information or secrets obtained need not be so damning to enable coercion. Westin notes that “every individual lives behind a mask,”\textsuperscript{368} or many masks, that are shown to the social audience. “If this mask is torn off and the individual’s real self bared to a world in which everyone else wears his mask and believes in masked performances,” the individual can be severely psychologically damaged.\textsuperscript{369}

Westin’s second underlying interest is emotional release. This, too, relates to the masks that people wear, or the varying roles they assume, with respect to separate audiences each and every day. Here, the issue is simply that being forced to wear any one mask or carry out any one role without relief is psychologically straining, and to do so indefinitely would “destroy the human organism.”\textsuperscript{370} Moments of respite are necessary to maintain a healthy psychological state. These moments of respite from playing socially demanded roles and complying with social norms also

\textsuperscript{365} \textit{R v Ward, supra} note 263 at para 61.
\textsuperscript{366} \textit{Westin, supra} note 239 at 32.
\textsuperscript{367} \textit{Ibid} at 33.
\textsuperscript{368} \textit{Ibid at} 33.
\textsuperscript{369} \textit{Ibid}.
\textsuperscript{370} \textit{Ibid at} 35.
allow individuals to carry out self-evaluation, the third of Westin’s underlying privacy interests. This is, in essence, the interest in being able to reflect upon events, process new information, and integrate these into the self in order to develop one’s identity as well as plan for the future.\footnote{Ibid at 37.}

The observation that individuals wear multiple masks and take on many different roles for varying audiences underscores much of Westin’s thought on the social value of privacy protection. This observation is directly applicable to anonymity on the Internet. Indeed, anonymity, and the related pseudonymity, can be seen as subversions of these masks or roles. By being anonymous, one avoids being associated with any particular social norms that might apply to a particular role or identity. Pseudonymity, meanwhile, allows the user to effectively choose his mask or role without the coercion of social expectations. By doing so, the user can better maintain his or her personal autonomy, and obtain respite from social pressures.

One issue that Westin does not address in detail, however, is the issue of identity. The wearing of masks and the assumption of roles invariably invites a discussion of the role of identity formation, but unfortunately, Westin does not discuss it. Indeed, there’s a close relationship between privacy and identity interests, which has been considered at length in the academic literature.\footnote{See e.g. Khan, supra note 140 (reviewing the history of this school of thought on privacy at 378-383).} In discussing the works of Edward Bloustein and Louis Henkin on privacy, Jonathan Kahn writes that:

\begin{quote}
Privacy is valued insofar as it fosters the conditions within which an individual may establish, maintain and develop her identity as a core aspect of personhood. Thus conceived, invasions of privacy constitute an affront to human dignity by undermining one’s identity.\footnote{Ibid at 382, discussing Louis Henkin, “Human Dignity and Constitutional Rights,” in Michael J Meyer & W A Parent, eds, The Constitution of Rights: Human Dignity and American Values 210 (Cornell University Press, 1992) and Edward J Bloustein, “Privacy As An Aspect of Human Dignity: An Answer to Dean Prosser” (1964) 39 NYU L Rev 962.}
\end{quote}

Professor Lisa Austin has similarly argued that the privacy interest in anonymity is tied to identity and identity formation through the ability to segregate audiences.\footnote{Austin, “Anonymous Blogging”, supra note 140.} In her view, anonymity and pseudonymity allow individuals to control their audiences and thus the social norms in which their messages will be received.\footnote{Ibid at 209-211.} Additionally, she has argued that much of
privacy law, particularly with respect to private law actions for privacy violations, are better conceived of as protecting the identity interest in self-presentation rather than particular harms or Kantian notions of personal autonomy.\footnote{Lisa Austin, “Privacy and Private Law: The Dilemma of Justification” (2010) 55 McGill LJ 165.}  

As these perspectives indicate, in a state of total observation and revelation, the individual becomes unable to develop her own identity. She is held to a single identity, known to all, and which becomes difficult or impossible to alter through a choice of modes of self-presentation. Perhaps worse, being held to a single identity for all purposes eliminates the ability for an individual to explore multiple parts of her personality or identity in different ways, and interferes with that individual’s interpersonal relationships. People have different personalities and different identities with respect to different audiences. Where those personalities and identities are forcibly combined into a single identity and single personality by breaching the individual’s privacy, a part of that individual’s sense of self, their personhood, is destroyed, along with the ability to control the terms of that person’s relationships. As Bloustein writes:

> A man whose home may be entered at the will of another, whose conversation may be overheard at the will of another, whose marital and familial intimacies may be overseen at the will of another, is less of a man, has less human dignity on that account.\footnote{Bloustein, supra note 373.}  

A person is less of a person when their privacy is lost through total observation or revelation because they are less able to define themselves and control their own bodies and thoughts. A number of commentators have reached this conclusion. Environmental Psychologist Irwin Altman believed that privacy was a process of social boundary formation that allows individuals to define that which is part of the individual self and that which is not.\footnote{Irwin Altman, The Environment and Social Behaviour (Monterey, California: Brooks/Cole, 1975) at 47-50.} Jeffrey Reiman, a professor of philosophy, took this conclusion one step further, arguing that:

> [t]he right to privacy is the right to the existence of a social practice which makes it possible for me to think of this existence as mine. […] [It] protects the individual's interest in becoming, being, and remaining a person.\footnote{Jeffrey H Reiman, “Privacy, Intimacy, and Personhood” (1976) 6:1 Philosophy & Public Affairs 26 at 43-44.}
Privacy, including anonymity and pseudonymity, is thus existential in nature: it is necessary to the definition and development of the self as an individual within a social context. Without privacy, we are defined entirely from without rather than from within. While identity is always partially defined in relation to others, without privacy, we lose the ability to have any control over who and what we are at any particular time or with any particular audience. Indeed, as will be discussed further in Chapter 3, privacy, like other personhood interests, is a necessary condition to being able to self-determine and self-define. It is more than political or social autonomy; it is the autonomy necessary to ontologically determine the boundaries between the self and the Other.

It is these fundamental personhood interests that underlie privacy and anonymity, and which the courts, when discussing online anonymity, were unable to identify. These interests also underlie the rigorous response anonymity has received on the Internet due to the unique ways the Internet affects them. The Internet has become a space in which, as anonymity and pseudonymity are normalized, new avenues of self-exploration, self-definition, and interpersonal interaction have opened up. This, in turn, has expanded our personhood interests in being able to self-determine in new ways.

One such way in which new avenues of personal growth and expression have been fostered on the Internet is the ability of the Internet to enable the wearing of masks and the assumption of roles that would not otherwise be possible to assume in the real world. Professor Gaia Bernstein has referred to the multiple masks we wear online as the fragmentation of identity.380 Similar to the notion of self-definition and self-determination discussed above, she sees identity as a “life-narrative,” or a story that we tell ourselves about who we are.381 To illustrate their importance, she refers to a clinical case of “Mr. Thomson,” who lost his long-term memory and was thus in a constant, near desperate, state of trying to invent a past in order to give meaning to his life.382 She identifies two often competing types of life-narratives, which she refers to as the “liberal” and “communitarian” “meta-narratives”.383 The “liberal meta-narrative” is the narrative that is the most common within liberal democratic societies, and it focuses on the freedom and

380 See Bernstein, supra note 8 at 986.
381 Ibid at 974-979.
382 Ibid at 994.
383 Ibid at 974-979.
autonomy of the individual to determine their own path in life and to self-define without conforming to social pressures. The “communitarian meta-narrative,” by contrast, is a narrative that focuses on the individual’s place in a community, and defines the self in relationship to the local society or culture in which the individual participates. It is less individualistic and more open to external normative pressures, and defines the self through group membership.\textsuperscript{384} The Internet, Bernstein argues, allows individuals to escape the meta-narratives that normally operate within a person’s life narratives. On the Internet, a person raised in a society with restrictive normative values, can, by using anonymity or pseudonymity, explore and express aspects of her personality that might be suppressed in her physical life, putting pressure on the communitarian meta-narrative, while expanding the liberal meta-narrative. At the same time, that individual may begin to find likeminded groups of individuals on the Internet that they may never otherwise have found, and thus become parts of new groups with new social norms, reintroducing the communitarian meta-narrative, although in a different form from the one of the society into which the individual was born.\textsuperscript{385} We hardly need to extend our imaginations very far to imagine that many LGBTQ persons may use the Internet to escape oppressive local social norms with respect to their gender identity or sexual orientation to find support and community among other LGBTQ persons.

Professor Bernstein notes, however, that along with the ability to reframe life-narratives in cyberspace by adopting different, or even multiple, identities, it can raise significant potential issues should they be disrupted.\textsuperscript{386} Indeed, she discusses how breaking the anonymity or pseudonymity of a user, especially where the user has constructed a very different identity from the one in real space, can have harmful effects not only upon the user, but also upon those who have come to know them through their online identity.\textsuperscript{387}

The harms of tying a pseudonymous identity to a real world identity are easy to understand through a simple example. Consider a man who interacts with others on an Internet forum devoted to women’s issues and self-identifies there as a woman and uses a pseudonym. Assume that he, through his female persona, has gained a number of online friends and established a

\textsuperscript{384} Ibid.
\textsuperscript{385} Ibid at 980-987.
\textsuperscript{386} Ibid at 986.
\textsuperscript{387} Ibid.
reputation as a meaningful contributor to the community. Should his online persona be tied to his real-life identity as a man, we can imagine that possible harms might follow.

The first, and most obvious, harm is that he may have his own real reputation damaged. People may object to his impersonation of a woman, possibly assuming he had nefarious intent. He may be mocked by those in the community around him, and his masculinity may be questioned.

The second harm is the harm to the forum community. Those who interacted with his persona may feel hurt or betrayed. The community may be damaged, with members unwilling to share their thoughts for fear that their group has been breached by unwanted outsiders. Of course, whether or not this is a harm that we would want to avoid by protecting anonymity is a normative question, since anonymity may lead to other members being less willing to participate out of fear that some of the members are not who they say they are. The view we take on this question would likely also vary depending on whether the other members’ reticence to participate with people under assumed identities is based upon legitimate concerns or prejudice. In either case, it remains a potential harm of destroying anonymity.

The third harm is that his own ability to express his identity online is compromised. He can no longer inhabit the female identity and express or explore that part of himself. Should he identify as female in his real life and feel unable to reveal that in his local community, these harms may be exacerbated. However, they may still exist even where the online female identity is merely a form of exploration or an expression of a smaller part of his personality. In either case, he may have a strong interest in continuing to function as a member of the community under his assumed identity. This harm arises not from reputational harm or fears about power and control, but rather from the loss of his ability to control his self-conception and self-expression. He can no longer be who he wants to be. In a psychologically real sense, he loses a part of himself and becomes less than he used to be.

Westin made similar observations with respect to the dangers of constant surveillance. Constant surveillance, he wrote, has enormous psychological impacts in that it forces the individual to attempt to constantly live up to standards and restrict his or her normal range of

\[388 \text{Ibid.} \]
\[389 \text{Ibid at 58.}\]
behaviour to only that considered acceptable in the circumstances. Bernstein might say that, here, the communitarian meta-narrative becomes overwhelming. Westin noted that such constant surveillance has been shown to have a “disintegrative effect” on social and group life.\textsuperscript{390} As the Internet enables constant surveillance of its users should the authorities or intermediary third parties wish to do so, some degree of protected anonymity is necessary to avoid the overwhelming social pressure that would apply under complete surveillance. This social pressure, in turn, would eliminate the ability to express oneself and develop in ways that might be defined as “human flourishing.”

Another important impact on identity and self-definition that arises from the Internet is the related ability of third parties to compile profiles of identity-defining information about a person without their knowledge or consent. Often referred to as “data mining”,\textsuperscript{391} these information compilers can be either descriptive or predictive. Descriptive data mining merely obtains and records the information given or obtained about a user. Predictive data mining, however, uses that information to infer new information. The predictive capabilities of data mining technologies are particularly worrisome, because they are capable of creating new, emergent data that not only records an individual’s online behaviour and information, but actively makes predictions about that person’s other information and future behaviour.\textsuperscript{392} In doing so, it begins to identify the individual’s psychological state, including that individual’s wants, fears, desires, and needs. Predictive data mining technologies thus represent not only a threat to one’s informational control, but of control over one’s identity and the ability to change it. The profiling power of predictive data mining technologies might be used by law enforcement and intelligence agencies to determine whether an individual is a threat, financial institutions might use it to determine who might be likely to default on a loan, search engines might use it to determine which results should be shown to a user, and retailers and service providers might use it to determine which items a consumer is likely to buy and which ones that person should be shown in advertisements.\textsuperscript{393}

\textsuperscript{390} \textit{Ibid} at 58-59.
\textsuperscript{391} Jason Millar, “Core Privacy: A Problem for Predictive Data Mining,” in Identity Trail, \textit{supra} note 14, 103 at 103-104.
\textsuperscript{392} \textit{Ibid} at 106, 111.
\textsuperscript{393} \textit{Ibid} at 106. For more on the dangers of data collection and profiling, see Frank Pasquale, \textit{The Black Box Society: The Secret Algorithms that Control Money and Information} (Harvard University Press, 2015).
However, the danger of predictive profiling goes beyond the very real concern that this information could be incorrect, or used in a way prejudicial to the individual’s interests. It potentially destroys an individual’s ability to choose who they are and who they can become. When used by third parties with the potential to either coerce or persuade an individual, the predictive profiling can become a self-fulfilling prophecy that leads a person to develop in a way consistent with the algorithmic predictions. If the only advertisements you ever see are for products that an algorithm thinks you might like, it’s probable that you’ll end up liking those things because the alternatives were never presented. The profile may have been accurate or inaccurate with respect to what you would have chosen absent those advertisements, but the result in either case is the same. And once this profile is established, it may be very difficult to change. This is especially true because the profile may slowly shift a person from his or her real preferences and desires towards the ones determined by the profile. As one article put it, “[t]he risk, however, is that our digital technologies may easily become defining technologies rather than mere identifying ones. They may move from being able to spot who we are to actually making sure that we become who they say we are, and do not change.”394 Predictive data technologies can be particularly insidious because they can capitalize on data that appears to be harmless or meaningless when disclosed. As that same article states with respect to information entered into search engines, “search engines easily distract us, making us believe that all we are doing is finding something we need, instead of uncovering ourselves as the kind of individuals who have such needs.”395 It is precisely these dangers to identity, autonomy and personhood against which anonymity and pseudonymity on the Internet provide at least some protection.

And the harms of the loss of anonymity or pseudonymity on the Internet are not trivial. Westin states that a loss of privacy generally can lead to nervous breakdowns, physical collapses, or even suicide.396 But these dangers are enhanced in the Internet context because of the special way in which the Internet both expands the ability to explore, determine and establish one’s identity, and the many ways that Internet technology can enable others to invade and limit those same identity interests. The Internet is thus a tool that can simultaneously be used to both

395 Ibid.
396 Westin, supra note 239 at 34, 41.
strengthen and weaken personhood. Privacy, and particularly anonymity, is key to ensuring that the latter does not overcome the former. If the law fails to do so, the consequences would be felt at a societal level. In the introduction to their book Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society, the editors write:

The ability or inability to maintain privacy, construct our own identities, control the use of our identifiers, decide for ourselves what is known about us, and, in some cases, disconnect our actions from our identifiers will ultimately have profound implications for individual and group behaviour […] It will affect the way that we think of ourselves, the way we choose to express ourselves, the way we make moral decisions, and our willingness and ability to fully participate in political processes.\(^{397}\)

Of course, total privacy is neither desirable nor possible. Westin notes that both having too much privacy—such as where one is trapped in total solitude—and having too little privacy can both be psychologically devastating.\(^{398}\) Maintaining a healthy psychological state thus require a balance between privacy and disclosure. However, he notes that our society tends to err on the side of disclosure over privacy,\(^{399}\) which is a concern that the courts and the legislatures should be cognizant of when crafting and interpreting privacy laws.

So is anonymity on the Internet, or at least the interests protected by anonymity on the Internet, truly unique? Does the response of the courts indicate the creation of unique digital rights or digital privacy interests? The law in Canada and the US has traditionally protected privacy where there is a “reasonable expectation of privacy.”\(^{400}\) One might suggest that the judicial opinions merely reflect the reality that, on the Internet, there is a reasonable expectation of privacy when operating anonymously or pseudonymously, whereas there is less of a reasonable expectation of privacy when going about one’s business in public in the real world. However, this argument is ultimately tautological. It would be reasonable to expect privacy where the law protects one’s privacy interests, and it would be unreasonable to expect it where the law does not protect one’s privacy interests. The fact that the Internet uses largely anonymous transfer protocols and that many websites allow for anonymous speech does not give rise to a reasonable expectation of

\(^{397}\) Identity Trail, supra note 14 at xxv.
\(^{398}\) Westin, supra note 239 at 41.
\(^{399}\) Ibid at 40.
privacy any more than does walking about wearing a hood. Indeed, the Supreme Court of Canada has recognized that a reasonable expectation of privacy is, in fact, a normative claim, which requires that there should be a protection for privacy interests rather than whether any particular person actually reasonably expected to enjoy privacy. Given the strong judicial response in favour of increasing privacy protections for anonymity online, it appears that much Internet conduct does operate within a space normatively giving rise to a reasonable expectation of privacy. The decision of the Privacy Commissioner of Canada with respect to personal information used for online behavioural advertising, discussed earlier in this chapter, similarly indicates a special respect for the importance of maintaining anonymity online. In my view, this treatment of privacy, and specifically, anonymity, arises from the unique ability of the Internet to both expand personhood interests such as identity formation and self-determination, and to undermine personhood interests by placing limits upon autonomy, freedom, and the ability of a person to be who they want to be in relationship to audiences of their choosing. In a sense, then, anonymity is a “digital right” not because it does not exist absent the Internet, but because of its special importance in the Internet context, and because of the unique ways in which it must be protected online.

b. Defamation, Copyright and Freedom of Expression

The Internet has become an incomparable tool for empowering individuals to express themselves and make their voices heard. From the ability of anonymous bloggers to discuss the most recent episode of their favourite reality television show to the power of repressed or underprivileged individuals to speak out against oppressive governments and regimes, the Internet has put the power to speak freely and openly to as wide an audience as possible into the hands of billions of people.

The argument that freedom of expression has been widely expanded as Internet access has grown is irrefutable, and it has become somewhat of a truism. Despite this observation, it does not follow that there is necessarily anything different in kind with respect to freedom of expression

401 R v Tessling, supra note 238. The United States’ jurisprudence is slightly different, requiring “a subjective expectation of privacy that society recognizes as reasonable”: Kyllo v United States, 533 US 27 (2001) at 33. In this, the US standard mixes a factual determination with one that might be considered normative.
402 OBA Policy, supra note 249.
403 See e.g. Ford, supra note 126.
on the Internet than there is elsewhere. We can take an entirely external view of the Internet and still see the potency of the Internet to be a tool for the wide dissemination of thought, ideas and information. Indeed, seeing the Internet this way is almost the very definition of the external view. While this perspective might see the Internet as perhaps the most powerful tool of expression and communication ever devised, this may well be merely a matter of degree, in the same way that one might see the telephone as merely different in degree from regular mail delivery. Taking this view, there is little reason to alter the existing protections regarding freedom of expression, nor its well-established limitations.

It is, of course, difficult to imagine significantly altering the general protections for freedom of expression, as they are already rather wide in both Canada and the United States. In Canada, freedom of expression is constitutionally protected under Section 2(b) of the Charter of Rights and Freedoms, which states that “Everyone has the following fundamental freedoms: […] (b) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication”.404 In the United States, freedom of speech is protected under the First Amendment to the Constitution, which states that “Congress shall make no law […] abridging the freedom of speech, or of the press”.405 Both of these clearly have a very wide ambit, at least with respect to protecting freedom of expression against government intrusions. However, naturally, the right to freedom of expression or speech is not absolute in either jurisdiction. It is the constitutionally-permitted limits on freedom of expression that truly define freedom of expression or freedom of speech jurisprudence.

Many of the constitutionally-permitted limits on freedom of expression fall under what would normally be considered freedom of expression or speech law. These limitations include hate speech (in Canada),406 obscenity,407 incitements to violence,408 and some instances of commercial advertising.409 However, in some cases, fields of law often considered discrete

---

404 Charter, supra note 334, s 2(b).
405 US Const amend I.
406 In Canada, prohibitions on hate speech are a valid limit on freedom of expression: R v Keegstra, [1990] 3 SCR 697. The United States, however, grants hate speech constitutional protection unless it that speech amounts to “fighting words”: Snyder v Phelps, 562 US 443 (2011).
408 See e.g. Chaplinsky v New Hampshire, 315 US 568 (1942).
409 See e.g. RJR-MacDonald Inc v Canada (AG), [1995] 3 SCR 199; Thompson v Western States Medical Center, 535 US 357 (2002).
practice areas serve as fundamental limitations on freedom of expression. These include copyright law\footnote{See e.g. Michelin, supra note 227; Sid & Marty Krofft Television Productions Inc v McDonald's Corp, 562 F (2d) 1157 (9th Cir 1977).} and defamation law.\footnote{See e.g. WIC Radio v Simpson, 2008 SCC 40, [2008] SCR 420; New York Times Co v Sullivan, 376 US 254 (1964).} It is these latter two areas of law that have received significant judicial and, in the case of copyright, legislative attention with respect to the Internet, and thus the areas that I will focus on.

As noted earlier, much of the response to the Internet within the realm of copyright has resulted simply from the fact that the Internet enables the reproduction and near instantaneous transmission of copyright-protected works at a near-zero cost. This has arguably upset the traditional balancing between the economic interests of the author and the public interest in dissemination of creative works.\footnote{See Gurry, supra note 214.} It has also undermined the foundational assumption that restricting the reproduction and distribution of copies will ensure economic returns to authors.\footnote{See Efroni, supra note 215.}

While this has led to a number of legislative and judicial responses that seek to address this balance, such as the enactment in Canada of legal liability for the circumvention of technological protection measures,\footnote{Copyright Act, supra note 213, s 41.1.} or the Supreme Court of Canada decision that attempted to ensure technological neutrality with respect to the duplication of royalty streams from songs,\footnote{Entertainment Software Association v Society of Composers, Authors and Music Publishers of Canada, 2012 SCC 34, [2012] 2 SCR 231.} some of the responses appear to attempt to protect, or even expand, freedom of expression online.

As mentioned in Part 2(e), above, these include the legislative expansions of fair dealing in Canada to include parody, satire, and education,\footnote{Copyright Act, supra note 213, s 29.} as well as the introduction of the non-commercial user-generated content exceptions to infringement.\footnote{Ibid, s 29.21.} As copyright inherently limits the ability of individuals to express ideas in certain ways,\footnote{See e.g. Michelin, supra note 227 (in which defendants were successfully enjoined from using a Michelin symbol on materials protesting the company’s conduct on copyright grounds).} any exceptions to those rules inherently expand freedom of expression.
These legislative additions to the exceptions to copyright infringement are noteworthy not only because they expand freedom of expression, but also for the way in which they do so. Explicitly recognizing new categories of fair dealing for parody, satire, and education\textsuperscript{419} demonstrates a respect for these forms of communication and the ways in which valuable speech can sometimes only be made effectively by using material that may be subject to copyright. It is very difficult to make a parody or satire of an existing work, for example, without potentially encroaching upon the copyright in that work, and obtaining a license in such circumstances may be highly unlikely. Fair dealing for educational purposes, similarly, recognizes that teaching can often best be done by using copyright-protected works, and that obtaining licenses for such works in all cases is unreasonable and potentially financially prohibitive.

It might be argued that these changes were a long time coming and that the Internet was not a primary motivating force behind their enactment. The process of enacting the \textit{Copyright Modernization Act} may merely have been a convenient process through which to review the state of copyright law generally and to enact changes that had long been considered. However, while this may partly be true, and while there were certainly discussions about expanding fair dealing outside of the Internet context,\textsuperscript{420} several factors suggest that these changes are indeed responses to the Internet. Firstly, it is important to recall that the \textit{Copyright Modernization Act}, which contained these legislative changes, was made expressly in contemplation of the societal and economic effects of the Internet.\textsuperscript{421} Secondly, and most importantly, the exception to non-commercial user-generated content, which immediately follows the expansion of fair dealing in the \textit{Copyright Modernization Act},\textsuperscript{422} and can be considered related, is clearly a direct response to the enormous culture surrounding user-generated content online.\textsuperscript{423} Indeed, this exception has often been referred to the as “YouTube exception” because of the ubiquitous presence of user-created YouTube videos that incidentally include copyrighted works, such as background music,\textsuperscript{424} although the provision isn’t limited to online activities.

\textsuperscript{419} Copyright Act, supra note 213, s 29.
\textsuperscript{420} See e.g. Michelin, supra note 227.
\textsuperscript{421} Copyright Modernization Act, supra note 63, preamble.
\textsuperscript{422} Ibid, ss 21-22.
\textsuperscript{423} See Hebb, supra note 230 at 238.
\textsuperscript{424} Ibid.
The non-commercial user-generated content exception is, of course, not absolute, as it only applies where the use is not for commercial purposes, the copyrighted work was legally acquired, the source or author is named if reasonable to do so, and the new work doesn’t negatively impact the market for the original.\textsuperscript{425} But despite the limitations, it’s quite an expansive provision that appears to recognize that the Internet has enabled enormous numbers of people to create, transform, communicate and consume creative works without any expectation of financial remuneration. It also views these activities as inherently beneficial enough to warrant creating (or at least confirming the existence of) an exception to copyright, and thus potentially devaluing authors’ economic rights in their works, in order to enable them. This view goes hand-in-hand with the observation that the Internet has also undermined the traditional assumption of copyright law that financial returns for authors are necessary to incentivize the creation of new works: an assumption which has widely been questioned, especially recently.\textsuperscript{426} Indeed, new creative works are created and distributed frequently through the Internet without an expectation of financial compensation.\textsuperscript{427} Because of the costs of production and physical distribution, engaging in this conduct was likely financially prohibitive prior to the Internet and therefore the number of people engaged in production without expectation of financial compensation was likely marginal. The non-commercial user-generated content exception thus represents a tacit endorsement of the non-commercial creative production enabled by the Internet.

The expansions to the explicitly enumerated categories of fair dealing can be read as similarly designed to promote the kind of communicative and amateur creative culture enabled by the Internet. While it’s possible to view them as expansions that might have been included in copyright reform legislation regardless of the Internet, the recognition given to Internet speech under the non-commercial user generated content exception suggests that the Internet played a significant role. Indeed, the Internet has given rise to vibrant community of fan-created works, such as fan fiction\textsuperscript{428} and machinima\textsuperscript{429} that may well be protected under the new exceptions for

\textsuperscript{425} Copyright Act, supra note 213, s 29.21.
\textsuperscript{426} See supra notes 235 and accompanying text.
\textsuperscript{427} See supra note 236 and accompanying text.
\textsuperscript{428} See Hebb, supra note 230.
\textsuperscript{429} Machinima refers to cinematic works made entirely within existing virtual worlds, such as video games, using the characters, art and landscapes of those worlds. See Rebekah Pure & Christopher Seaman, “The Problem of the Parody-Satire Distinction: Fair Use in Machinima and Other Fan Created Works” (2012) 3 U Balt J Media L & Ethics 171.
parody and satire, even where those works are used for commercial purposes.\textsuperscript{430} By expanding
fair dealing to encompass these types of creative expression, Parliament may be attempting to
promote the very kinds of content creation and distribution that the Internet has enabled.

While copyright has been altered by legislative amendments, defamation law has not been the
subject of any similarly direct changes. However, like copyright, defamation is traditionally
viewed as a special category of legitimate restriction on freedom of expression,\textsuperscript{431} and one that
has been significantly challenged by the Internet. Here, however, the challenge has come in
balancing the right to freedom of expression with the ongoing interest of individuals in
protecting their reputations. As discussed earlier in this Chapter, this balancing is made difficult
by a combination of the use of anonymity and pseudonymity by defamers, the widespread and
permanent nature of much Internet speech, and the ability of various organizations and
individuals to attempt to silence online speech through the use of cyberSLAPPs. The Internet
thus shifts the balance in strange ways, putting some additional power in the hands of both sides
of the defamation equation while often leaving some victims of defamation without a remedy.\textsuperscript{432}

Fortunately, the law’s response to this has not been to immediately jump to the protection of
plaintiffs by making it easier for them to both identify and bring action against alleged defamers.
While the courts have recognized that online defamation can be especially pernicious due its
wide distribution, relative permanence, and the possibility of being taken more seriously in
certain online contexts,\textsuperscript{433} courts in both Canada and the United States have attempted to ensure
that they maintain a strong protection for freedom of expression against frivolous claims and
cyberSLAPPs. In Canada, this has meant that, before a court can order a third party to release
identifying information of an anonymous alleged defamer, the plaintiff must show a \textit{prima facie}
defamation case and must point to the precise statements made.\textsuperscript{434} Indeed, the Ontario Divisional
Court warned against the possibility of a “chilling effect on freedom of expression”\textsuperscript{435} from a

\begin{itemize}
  \item \textsuperscript{430} See Hebb, \textit{supra} note 230 at 246-247.
  \item \textsuperscript{431} See \textit{supra} note 411.
  \item \textsuperscript{432} See Richards, \textit{supra} note 6 at 523-524.
  \item \textsuperscript{433} See e.g. \textit{Barrick Gold Corp v Lopehandia}, \textit{supra} note 267.
  \item \textsuperscript{434} \textit{Warman v Wilkins-Fournier}, \textit{supra} note 265 at para 42.
  \item \textsuperscript{435} \textit{Ibid.}
\end{itemize}
failure to properly balance reputation and freedom of expression and suggested that “a more robust standard is required [than that of BMG v. Doe].”  

Some courts have gone even further in the US context, requiring not only that a *prima facie* defamation case be made out, but also that the court balance the strength of that *prima facie* defamation case against the First Amendment rights of the alleged defamer. Not all US courts have embraced this balancing, however, and the approach to anonymous defamation remains a patchwork across the United States.

What is, however, clear is that with respect to both copyright and defamation, the courts and the legislatures—at least in Canada—are attempting to support the unique nature of speech on the Internet. Indeed, the Internet has given a voice to millions of people and levelled the playing-field with respect to the cost of broadcasting and transmission. An individual of extremely limited resources with access to a computer and the Internet at a library could potentially gain a reader base of millions and become widely influential. The Internet opens up opportunities for people to express themselves that never otherwise would be available, democratizing discourse on everything from politics to religion to consumer goods to entertainment.

Two important elements of the unique nature of speech on the Internet are that it is participatory in that it enables a constant conversation rather than a one-way communication, and that it is often amateur, in that the people doing the talking are often not professionals, nor can be expected to be familiar with the complexities of copyright law or defamation. The law has thus attempted to respect the importance of this participatory nature, and understand its often amateur bent, while still ensuring some level of accountability.

This respect for amateur and participatory speech on the Internet clearly implicates respect for the ways in which the Internet affects the personhood interests of Internet users. There is little debate that freedom of expression is a personhood interest, at least insofar as the autonomy to live one’s life in accordance with one’s purpose and to develop as a human being can be...
considered a personhood interest.\textsuperscript{441} Indeed, it is so fundamental to one’s freedom, autonomy, and ability to be an individual in society that Justice Rand of the Supreme Court of Canada said in 1957 that it is "little less vital to man’s mind and spirit than breathing is to his physical existence".\textsuperscript{442} Justice Cardozo of the United States Supreme Court held it in a similarly high regard, stating that freedom of speech is "the matrix, the indispensable condition of nearly every other form of freedom".\textsuperscript{443} These statements are true irrespective of speech on the Internet, but Internet speech does appear to warrant a special level of protection, indicated by the way it has spurred changes in both the defamation and copyright contexts. Indeed, in the United States, there is highly persuasive judicial \textit{dicta} for the idea that Congress cannot regulate speech on the Internet, whereas it can in other media such as broadcast telecommunications.\textsuperscript{444} This is because the Internet is “the most participatory form of mass speech yet developed,”\textsuperscript{445} it has very low barriers to entry for both speakers and listeners, it creates a “relative parity” between Internet users, and because it contains “astoundingly diverse content.”\textsuperscript{446} Additionally, unlike many broadcast communication media, there is no scarcity of broadcasting resources, and thus there is practically no limit to the number of people that can speak, nor the amount of content that can be transmitted, on the Internet.\textsuperscript{447}

There are, of course, some countervailing developments. For example, a recent study demonstrated that the United States’ notice-and-takedown regime for claims of online copyright infringement has led to a proliferation of automated content takedown systems that have little human oversight.\textsuperscript{448} Because of the lack of human involvement, and the resultant lack of a proper determination of whether any copyrights were actually infringed, such systems may be seen as legislatively motivated systems that undermine free speech by giving priority to claims of copyright infringement over the interest in free expression. Despite such countervailing trends,

\textsuperscript{442} Switzman v Elbling, [1957] SCR 285 at 306.
\textsuperscript{443} Palko v Connecticut, 302 US 319 (1937) at 327.
\textsuperscript{444} Reno v American Civil Liberties Association, 521 US 844 (1997) at 863.
\textsuperscript{445} Ibid.
\textsuperscript{446} Ibid.
\textsuperscript{447} Ibid at 870.
however, in my view it’s undeniable that the Internet has massively expanded the opportunities for free expression, and that the law has, by-and-large, protected these interests.

This is understandable. No medium before has democratized expression so completely, nor made accessing the speech of others so immediate and efficient. Because this has led to a proliferation of creative content, amateur expression, democratic discourse, and general social and civil engagement, it stands to reason that the law should stand to protect it. Freedom of expression is fundamental to autonomy and personhood. Without it, individuals would be unable to hear all views and thereby seek the truth, nor find the information that may be vital to their own personal development. They cannot develop their judgment and sense with respect to the information they receive. And they cannot say what they want to say, destroying their ability to define and express their own identity and to carry out their own ends in a social universe.449 Both the freedom of receive unfettered speech and to speak without limitation are therefore vital to the self-definition and autonomy that are vital to personhood, and as the Internet has vastly expanded the ability to speak, so too has it vastly expanded the personhood interests of its users. In that sense, freedom of expression is a “digital right” insofar as it creates a uniquely participatory level of speech and engenders new creative works, and therefore appears to receive a special level of protection in the Internet context.

c. Email Spam

Email spam has been a growing problem since Internet users, businesses and others began receiving it in large quantities during the 1990s.450 As noted earlier in Part 2(h), the American courts were the first to address the concerns raised by users and businesses, largely through the common law tort of trespass to chattels,451 although other methods, such using nuisance law,452 were proposed. Later, states addressed it through local legislation,453 and then, later still, the United States Congress passed the CAN-SPAM Act.454 In Canada, there was little judicial or

449 See generally Moon, supra note 441 (generally reviewing the various reasons to protect freedom of expression).
451 See supra note 289.
452 See Kam, supra note 27.
453 See supra note 292-293 and accompanying text.
454 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, supra note 294.
legislative action related to spam communications until the passage of CASL in 2010, although CASL contains spam regulations much broader and more limiting than those seen in the United States.

As I’ve briefly reviewed the content of these provisions earlier in this Chapter, I will refrain from doing so again here. Here my concern lies with defining the harms of email spam that these laws seek to address. Given the widespread adoption of laws attempting to limit the sending of email spam, and extensive punitive measures such as CASL’s maximum administrative monetary penalty of ten million dollars for organizations, it’s clear that the perceived harm created by email spam is significant.

Most commentators when discussing the harms of email spam focus on the economic consequences. These harms are not to be taken lightly. Indeed, in a paper by research scientists Justin Rao and David Reiler, from Microsoft and Google respectively, estimated in 2012 that email spam cost consumers and businesses twenty billion dollars. In 2010, they note that an estimated 88 percent of all email traffic was spam.

Spam is particularly pernicious because it is a marketing method in which the vast majority of its costs are borne by consumers as externalities. That is, it costs very little for spammers to send unsolicited commercial messages, but it costs a lot for users and businesses to sort through spam, and for technology companies to develop and implement filtering mechanisms. Indeed, without these filtering methods, many email inboxes might be rendered useless. While the vast majority of spam is either blocked by automated spam filters or deleted by users, and the majority of spam actually read will be ignored, due to its low costs, even an incredibly low conversion rate will still more than justify the expense. Spam is thus a prime example of how a

\footnotesize

455 CASL, supra note 60.
456 See e.g. Kam, supra note 27; Zhang, supra note 450; Thomas K Ledbetter, “Stopping Unsolicited E-Mail: Why the Can-Spam Act is Not the Solution to Stop Spam” (2004) 34:1 Sw U L Rev 107.
457 Rao & Reiler, supra note 285 at 88.
458 Ibid at 87.
459 Ibid.
460 Ibid at 88.
461 Zhang, supra note 450 at 304.
technology can enable an activity with large externalities that need to be internalized or limited through legal action.

The low cost of spam separates it from other media through which unsolicited messages might be sent. For example, sending the same volume of messages through the traditional post would be orders of magnitude more expensive.\textsuperscript{462} This may explain why there is little legislative activity regulating unsolicited advertising mail through regular postal services. Another reason may be that postal delivery is primarily a state monopoly in both Canada and the US, meaning that controls on such advertising mail can implemented through internal postal service policy rather than public legislation. For example, in Canada, Canada Post will not deliver unaddressed advertisements if the recipient simply posts a note indicating their desire not to receive such solicitations on his mailbox, although this will not affect commercial messages addressed to the recipient.\textsuperscript{463}

Despite the clear economic harms of spam, there are indications that the harms of electronic spam communications goes beyond the financial to the personal. The first indication is the powerful emotional reaction that people have to spam. Spam has been described in professional publications as “viscerally offensive to the general public,”\textsuperscript{464} and “an egregious intrusion of online space, and […] a pernicious evil to Internet usage.”\textsuperscript{465} These do not sound like criticisms levied at conduct with merely economic externalities. These instead sound like lamentations of a harm more akin to nuisance or the invasion of personal privacy.

Professor Andrea Slane has written that the right not to receive spam communications is ultimately about personal autonomy.\textsuperscript{466} She compares one’s autonomy interests in one’s virtual presence to one’s autonomy interests while in the physical home, which has long been protected in US jurisprudence.\textsuperscript{467} Indeed, US Courts have long viewed the receipt of unwanted

\textsuperscript{462} Ibid.
\textsuperscript{464} Slane, \textit{supra} note 284 at 263, quoting Campbell, \textit{supra} note 287 at G5.
\textsuperscript{465} Hunter, \textit{supra} note 147 at 478.
\textsuperscript{466} Slane, \textit{supra} note 284.
\textsuperscript{467} Ibid at 264-269.
communications in the home as a violation. Slane cites Justice O’Connor of the Supreme Court of the United States, who once wrote:

> a special benefit of the privacy all citizens enjoy within their own walls, which the State may legislate to protect, is an ability to avoid intrusions. Thus, we have repeatedly held that individuals are not required to welcome unwanted speech into their own homes and that the government may protect this freedom.\(^{468}\)

Professor Slane suggests that we expect a zone of privacy around our Internet use, and particular our email inboxes, similar to the way we conceive of the home. She argues that spam communications violate that private space, and thereby impact our autonomy interests.\(^{469}\) She does not suggest that the email inbox is a “home” in any property or real sense, or even that we expect to normally access our inboxes from our homes, but rather that the notion of the home represents a protected space in which one can exercise their autonomy interests. Thus, in her view, some areas of the Internet, like the inbox, are personal and private areas in which we expect autonomy in a similar manner to being within our homes, and deserve similar levels of protection.

Jeremiah Kelman has argued along similar lines, stating that:

> More than any other virtual space on the Internet, the inbox has an exclusive quality (at least in the perception of Internet users) comparable to the absolute dominion traditionally bestowed on one’s home […] partly because] the inbox […] is socially perceived as an invitation-only medium. […] Upon recognizing the essential quality of one's inbox as a communicative medium connecting occupants of real property, one can then reasonably view the e-mail account itself as a fixed aspect of real space. […] In this way, the inbox can be viewed either as a fixed (or at least, semi-fixed) conduit into real property or an inherent part of residential use itself.\(^{470}\)

This view of the inbox as analogous to the home is understandable given the role, discussed earlier, of the Internet in personal autonomy, identity formation, and personhood. As the Internet is a vehicle through which personhood can be manifested and expanded, some areas of the


\(^{469}\) Slane, *supra* note 284.

Internet must be free from intrusion in order to ensure that the individual retains the necessary freedom to pursue their own interests. In this, the metaphor of the home is apt, as the home has long been protected as a space in which a person is free to pursue her own ends without interference, to seek solitude or intimacy, or to engage in self-fulfilling behaviour without the need to conform to social norms.471 The home is not protected because of anything to do with its particular location or method of building; it is protected because of what it allows people to do and what it represents to them. Ultimately, therefore, it is the human experience of people with respect to the home that is relevant. The same can be seen as true with respect to the Internet.

In this, an obvious comparator is that of intrusive telemarketing calls. Both Canada and the United States have established federal frameworks to address telemarketing, including national Do-Not-Call Lists and prescribing specific conditions for telemarketing.472 Unlike email spam, telemarketing typically has high costs due to the requirement to have an agent on the other end of the call, and the ability to make only a limited number of calls. Additionally, the externalities are less of a concern, because there is little danger of overwhelming any technical systems by making a high volume of calls. Nonetheless, statutory responses have been made to limit the intrusive effect of these calls based on the right not to be interfered with in the home and a respect for personal privacy that is operative in that context.473 As electronic spam can be considered at least somewhat analogous to unwanted telemarketing calls, it’s clear that privacy interests are also operating in the email context. This is also visible in the early calls by commentators and legislators to address spam through nuisance,474 which is more commonly associated with intrusion or trespass than economic harms.

Another reason to see the harm of spam as separate from its economic effects and its potential impact upon technological systems is that many complain of the content of the messages rather than the mere existence of the messages themselves. If the harm was only economic and technological, the content would not matter. However, it’s clear that the content does matter.

473 Slane, supra note 284 at 277.
474 See ibid (describing early legislative attempts in Canada at both provincial and federal levels to address spam as a form of nuisance at 274). See also Kam, supra note 27; Lemley, supra note 164 at 540.
While the fraudulent nature of spam communications is often cited as a primary concern,\(^{475}\) many are troubled with the personal and intrusive nature of the content.\(^{476}\) One Canadian Senator, cited by Professor Slane, put it as follows:

> I do not believe Canadians would tolerate pornographic magazine subscriptions or free edible underwear samples turning up in their traditional post each morning. I do not believe they would appreciate seeing their preteen daughter’s name on the address box of a coupon book for diet pills and breast enhancements. I do not believe for a second Canadians would allow such damaging messages to enter their homes, yet this is precisely what occurs over the Web.\(^{477}\)

Statements of this nature, as well as examples of individuals who have felt slighted by the contents of unsolicited advertisements,\(^{478}\) suggest that more than mere economic effects are at stake. Indeed, they suggest spam can amount to a personal affront.

Writing before the enactment of CASL, Professor Slane suggested a number of possible legislative schemes through which to address the autonomy implications of spam. She recommended both an administrative remedy in which complaints could be made to a coordinating and enforcement body that could then take action against the alleged spammers.\(^{479}\) She also recommended a private right of action available to individual spam recipients that would allow them to bring their own grievances directly against spammers, largely as a symbolic gesture.\(^{480}\) The fact that Canada’s CASL implements precisely these measures further indicates that autonomy interests are being considered in the legal response to spam.

I certainly do not want to suggest that the only reason spam has been addressed legislatively is because of this sense of invasion or the affected autonomy interests. Its economic harms remain real and important. However, like in the legislative responses to receiving unwanted marketing telephone calls, autonomy interests appear to be a factor to which the law has responded. While

\(^{475}\) See e.g. Zhang, *supra* note 450 at 311; Ledbetter, *supra* note 456 at 111.

\(^{476}\) Slane, *supra* note 284 at 277.

\(^{477}\) *Ibid* at 264, quoting Senator Donald Oliver in *Debates of the Senate (Hansard)*, 37th Parl, 2nd Sess, No 140, Issue 77 (24 September 2003) at 1530 (Hon Donald H Olivier).

\(^{478}\) Professor Slane refers to the case of Charles Booher, a penile cancer survivor who felt so frustrated and slighted after receiving numerous penile enhancement spam messages that he resorted to personal threats against the president of the company responsible. *Ibid* at 261.

\(^{479}\) *Ibid* at 284

\(^{480}\) *Ibid.*
the significantly higher penalties contained in anti-spam legislation like CASL\textsuperscript{481} may be a result of the economic externalities created by spam, other aspects, such as the private right of action,\textsuperscript{482} suggest that privacy, autonomy, and thus, ultimately, personhood interests are implicated in the legal responses to the rise of spam.

The nature of the personhood interest on the Internet, and how it relates to a theory of legal adaptation to the Internet will be explored in the next Chapter.

\textsuperscript{481} CASL, supra note 60, s 20(4).
\textsuperscript{482} Ibid, ss 47-51.
Chapter 3
Personhood as a Substantive Theory of Legal Adaptation to the Internet

1. Chapter Overview

In the previous Chapter, I identified personhood interests as the motivating force behind a number of legal adaptations to the Internet. These personhood interests include anonymity and control of identity, freedom of expression, and security against limits on individual autonomy. I also argued that these interests have been uniquely impacted by Internet technology, and thus have given rise to unique legal responses, which I have termed “digital rights.” While these “digital rights” are extensions of rights recognized previously either by the law or by legal scholars, in my view, these rights take on new and distinct meanings in the online context. In this Chapter, my aim is to explain the special relationship between the Internet and personhood that gives rise to these rights, and by doing so, develop a substantive theory of legal adaptation to the Internet. This theory asserts that the Internet offers users expanded opportunities to develop one’s own identity and self-conception, and to pursue one’s own purposes, ultimately assisting individuals in fostering their own personhood. A working definition of “personhood” is required for this theory, which I address in Part 2 by reference to philosophical accounts of the self, including existential self-determination and Kantian freedom. This leads to an account of the Internet, discussed in greater detail in Part 3, as a medium that can facilitate both the expansion of personhood and limitations upon personhood, creating a need for sort of “digital rights” reviewed in Chapter 2 to ensure that personhood interests are protected in the online environment.

The effect of the Internet upon personhood interests suggests a number of implications, discussed in Part 4 of this Chapter. Firstly, I discuss striking a proper balance of regulation on the Internet between protecting users’ personhood interests and ensuring that the Internet is not freely used to infringe the traditional rights of others. Secondly, I discuss the issue of virtual property in virtual worlds, and consider how the personhood interests of users affects the debate concerning whether property rights should manifest in virtual property. Thirdly, I address the—largely
hypothetical—issue of whether there might be a valid cause of action for the defamation of a pseudonymous identity, and thus whether one has a right to a reputation in a pseudonymous identity. Finally, I consider how the personhood interests identified by this theory of legal adaptation to the Internet impacts the debate about whether the Internet could be considered a human or fundamental right, as well as the tangentially related issue of net neutrality.

2. A Conception of Personhood

Until now, I have assumed a general understanding of the term “personhood,” as well as the related definitions of words such as “autonomy” and “harm.” However, to fully develop personhood a substantive theory of legal adaptation to digital technology, it is necessary to further investigate the nature of personhood, and what it means to have autonomy or freedom, and what it means to be harmed.

The Oxford English Dictionary defines “personhood” as “the quality or condition of being a person; esp. personal identity, selfhood.” It is thus more than merely the prosaic and everyday identification of a human being as a person. In that conception, a person, to be a person, need not have anything other than his own mind and body, and the term is thus an objective one. Here we are concerned with the qualities and conditions that define a person’s identity and selfhood; those attributes that allow a person to be a moral agent, to make decisions, and to interact with others and function in a society of persons.

In this sense, we need to differentiate the term “personhood” as used here from another of its more common usages as denoting the subject of legal rights. This latter usage is common with respect to, for example, corporate personhood or, historically, the personhood of women. In these cases, entities with “personhood” are those that can be considered to have the rights normally granted to ‘persons’, such as freedom of expression for corporations, or the right to hold certain official offices for women. In this Chapter, we are concerned with a more fundamental

483 The Oxford English Dictionary, OED Online, sub verbo “personhood”.
484 Notwithstanding the hypothetical question of whether a consciousness contained in a medium outside of a human biological form is a ‘person.’
485 See e.g. RJR-MacDonald Inc v Canada (AG), supra note 409 (concerning the freedom of expression of corporations with respect to commercial speech).
486 Edwards v Canada (Attorney General), 1929 UKPC 86, [1930] AC 124 (concerning whether women were ‘qualified persons’ for the purposes of holding a seat in the Canadian Senate).
question of what attributes are necessary for an entity to be considered a ‘person,’ and what freedoms and resources are necessary to allow a person to continue to be and function as a person within both the real world generally and within modern society. The attachment of legal rights and obligations to persons is often a means of ensuring that those attributes, freedoms, and resources are protected, but questions of corporate personhood or the personhood of specific categories of human beings presuppose an existing definition of ‘person,’ and thus ‘personhood,’ of the variety being discussed here.

In order to be consistent with the somewhat empirical approach taken in this thesis, the concept of personhood reflected here must be one that is responsive to manner in which the courts have considered various interests to be fundamental to the person, such as privacy and freedom of expression, and the ways in which they associate these interests with notion of personal development, fulfilment and flourishing. For example, the Supreme Court of Canada has identified “individual self-fulfillment and human flourishing” as a central value protected by freedom of expression. With respect to privacy, the Ontario Court of Appeal has stated that “[p]ersonal privacy protects an individual's ability to function on a day-to-day basis within society while enjoying a degree of anonymity that is essential to the individual's personal growth and the flourishing of an open and democratic society.” Any definition of personhood must capture this notion of the person as one capable of growth and flourishing, rather than merely a static definition of a thing that is.

The philosophical canon holds a number of distinct views concerning the definition of a person. John Locke’s view was that a person is "a thinking intelligent being, that has reason and reflection, and can consider itself as itself, the same thinking thing in different times and places." This view, however intuitively true, fails to offer a reason to protect many of the rights considered fundamental for persons to function as persons. Locke’s view of the person offers no reason to intrinsically protect freedom of expression or privacy. His definition is so naturalistic as to demand nothing more than the innate qualities of the human consciousness.

487 Irwin Toy v Quebec (Attorney General), [1989] 1 SCR 927 at 976.
488 R v Ward, supra note 263 at para 71.
Immanuel Kant, meanwhile, postulated the person as a rational being “whose actions can be imputed to him”⁴⁹⁰ and who is the “subject of a morally practical reason.”⁴⁹¹ Kant thus views the person as an abstract rational being, largely defined in relationship to others. While Kant attributed the fundamental right of freedom to every human,⁴⁹² in his conception this right follows from the fact of one’s humanity rather than composing it. This, too, does not get us much closer our objective of reaching a more substantive theory of personhood. It is not that these theories are necessarily flawed, but rather they do not go far enough. Even if we combine the theories presented thus far to say that a person is an intelligent, thinking, human being, who can consider itself as itself, understands the continuity of its own existence, and whose acts are imputable to itself, we still cannot justify the protection of freedom of speech, privacy, or even protections from physical restraint as necessary to personhood. A human trapped in chains, subject to constant and intimate observation, and without the ability to communicate would still have as much “personhood” as anyone alive. Moreover, these conceptions fail to address the person as a changing thing, capable of self-development, growth and flourishing.

The concept of personhood as containing elements of constant self-development and growth is perhaps closest to the ideas articulated by existential philosophers. Jean-Paul Sartre often used the well-known phrase “existence precedes essence” to define what was meant by a person, or ‘man’, within existential thought.⁴⁹³ Indeed, he called this the “first principle of existentialism.”⁴⁹⁴ Put simply, the principle means that an individual first materializes in the world (the existence), “encounters” herself, and only after existing can she define herself, or her “essence”.⁴⁹⁵ Existential thought thus represents a denial of strict universal notions of the essence of a person, or any universal idea of human nature.⁴⁹⁶ Instead, people are in a constant state of defining themselves, and a person is always “not yet.”⁴⁹⁷ Existentialism as a whole arises out of

---

⁴⁹¹ Ibid at 186.
⁴⁹² Ibid at 30.
⁴⁹⁴ Ibid.
⁴⁹⁵ Ibid.
⁴⁹⁶ Ibid.
the realization of the absurdity, emptiness and pointlessness of the universe,\(^{498}\) or, as Sartre noted, the non-existence of a God who could otherwise give some higher order and meaning to the world.\(^{499}\) Instead, the person faces a world inherently devoid of meaning, and the only one who can give any of it meaning is the self. While the natural sciences can reach objective conclusions concerning what is, they are incapable of giving anything meaning, or of determining moral right and wrong, and thus they are incapable of guiding human action. Thus, only the person can create her own morality, and give meaning to her life and the world in which she exists.\(^{500}\) Only by creating one’s own purposes and following through on them with sincerity can one live a fulfilling and authentic life.\(^{501}\)

Existentialism thus offers a way around Hume’s is/ought problem. The is/ought problem, perhaps most famously articulated by David Hume,\(^ {502}\) is that it is impossible to logically derive any arguments about what ought to be from observations about what is. In other words, we cannot find any moral truths, articulate any notion of the good, or create any normative arguments based solely upon empirically observed facts. For example, the statement “he will die if I do not help him, so I ought to help him” is not logically consistent. It may be objectively true that without my intervention a person will die, but it does not logically follow that I therefore ought to help him. In order for the statement to be logical, one must first articulate a goal or a moral judgment. The statement “he will die if I do not help him, and I wish to prevent the death of others, so I ought to help him” is a logical statement. But it requires an individual goal (e.g. I aim to prevent the deaths of others) or a moral judgment (e.g. interceding to prevent the death of others is moral good or duty) that can never be derived from pure reason and empirical observation alone. Existentialism offers a way out of this conundrum by simply saying that one must create their own moral rules, define their own meaning, and establish their own goals. These are based not solely on reason, but on the subjective determinations by the individual about who she is and who she will be.

---

\(^{498}\) Ibid at 508.

\(^{499}\) Sartre, supra note 493 at 28-29.

\(^{500}\) Ibid at 29-30.

\(^{501}\) Ibid at 46-51.

Existentialism is not, however, divorced from reality. An individual cannot choose to be, for example, a dolphin, by the exercise of their will. Indeed, existentialists refer to the limitations of one’s reality as one’s “facticity”. Regardless of one’s facticity, a person has the ability to “transcend” by reflecting upon those limitations to give them meaning and purpose. Indeed, existentialism is focused upon the inherent freedom of the person to self-define and self-determine. This freedom is at once a great source of optimism, but also a deep source of anxiety, in that this freedom to choose one’s own self and life without any exterior guidance also comes with an overwhelming responsibility for oneself. Like the legal responses to the Internet focused upon in Chapter 2, existential thought is concerned with a sort of “interior view” of the lived experience and the subjective understanding of the world rather than the detached and objective perspective of the natural scientist. It tends to privilege subjective truths and beliefs over objective and scientific knowledge.

Existential theory helps us understand the concept of the person that the courts imply when justifying basic rights such as privacy or freedom of expression on the grounds of personal growth and fulfilment. If persons are endlessly self-defining, and must be to live any kind of meaningful or fulfilling life, this leads us to an understanding of personhood as both the freedom to engage in, and the state of, constant self-determination and self-development towards whatever purposes have been set by the individual.

I note that I take existentialism only so far. I do not, as some existentialist do, reject the Cartesian mind-body duality, nor privilege subjective knowledge over objective knowledge or empirical evidence. Existential notions of “authenticity” are also largely unhelpful. Rather, I merely

---

503 Aho, supra note 497 at 52-53.
504 Ibid.
505 Ibid at 63.
506 Ibid at 73.
507 Ibid at 23-25.
508 Ibid at 35-36. The notion that existence precedes essence is not incompatible with the Cartesian mind/body duality. Sartre does take the Cartesian ‘cogito’ (“I think therefore I am”) as his starting point for existential thought (Sartre, supra note 493 at 40), but his rejection of the mind-body duality appears to go beyond existentialism’s core premises, even if he considers it essential to his views.
509 Ibid at 35. In my view, both types of knowledge are equally important. Objective knowledge allows us to understand the world with some degree of certainty and predictability, while subjective knowledge allows us to determine what is important, what is good, and what goals we should set for ourselves. Both are equally necessary for persons to live.
510 Authenticity” is often described as being true to oneself and not merely conforming to outside pressures on what to do and what roles to adopt. It requires sincere self-reflection and responsible self-direction resulting in positive
take existentialism for its central point that the person is a self-defining creature that has the freedom to choose her own ends and give meaning to the world, and that she must do so in order to live a satisfying life. Thus, personhood is the state of freedom in which one is able to determine and pursue one’s own identity and one’s own purposes.

My conception of personhood as a form of freedom does differ somewhat from the existential conception of freedom, however. Existential freedom is often seen a freedom of intention; it is inherently internal rather than being affected by external realities. Even being in a state of slavery does not undermine it since the slave is still free to choose his intentions and his meanings within the objective context of his existence, even if he is more limited in his ability to act.\textsuperscript{511} In my view, this does not follow. All people are limited, even in their intentions and thoughts, by what they know and what they know to be possible. Without external information and the ability to process it, we can neither think nor intend. A slave who knows his chains to be unbreakable by any means available to him cannot reasonably intend to be free, nor can he intend to be a university professor. Even his world of intention is rendered more limited. Neither is a person lacking in the necessities of life completely free to intend or create meaning, as obtaining the necessities of life must always be a prior purpose, imposed by external forces, before he is free to intend anything else. A dead man cannot intend nor act upon those intentions. Personhood thus requires external factual freedoms before it can be realized in full.

The existentialist viewpoint used here is only intended to serve as an exposition helpful in understanding personhood as a richer concept than mere existence or the entity to which legal rights can be ascribed. However, existentialism is not necessary to understanding personhood in this way. Indeed, the many ways in which this examination of personhood diverges from some traditional existentialist thought indicates that I take only that from existentialism that is congruent with the viewpoint taken here, rather than grounding the analysis fully within existentialist thought.

\textsuperscript{511} Ibid at 72-73.
Indeed, it is, I believe, also possible to ground a similar, but perhaps not identical, conception of personhood upon Kantian notions of freedom. Kant considers freedom to be “the only original right belonging to every man by virtue of his humanity.”\textsuperscript{512} This freedom exists in two modes: inner freedom and outer freedom. Inner freedom relates to freedom from coercion, or from having one’s own freedom to pursue their ends without interference from others.\textsuperscript{513} Outer freedom, on the other hand, consists of the freedom to choose one’s own ends, and thus cannot be either externally legislated or meaningfully interfered with.\textsuperscript{514} Kant postulates these freedoms as a form of original right belonging to humans rather than something inherently constitutive of persons,\textsuperscript{515} and therefore freedom itself cannot necessarily be conceived of as a form of personhood. In other words, one’s degree of either internal or external freedom, in Kant’s view, does not give rise to a change in one’s capacity to be a person. Indeed, internal freedom will always be unencumbered by the actions of others, and Kant assumes that all people inherently possess a conscience capable of exercising such freedom.\textsuperscript{516} Limitations on external freedom, likewise, do not constitute a loss of personhood, but rather merely a wrong committed by the responsible party.\textsuperscript{517} Nonetheless, Kant views a person as a human being that is to be respected as an end in himself,\textsuperscript{518} and not one to be used for one’s own ends. In this sense, the notion of a person is largely defined by the relationship between a person and other persons. As Kant also sees freedom as an innate right, we can conceive of a sort of Kantian personhood consisting of the relationship of respect between human beings that protects the innate freedom of persons. As persons have an obligation to choose and pursue their own ends,\textsuperscript{519} a respect for freedom as an innate right must also implicate a respect for acts of self-determination. In this, then, personhood is not the freedom to self-determine, but rather the respect and non-interference granted to that freedom by others. This conception of personhood, like Kant’s definition of a person, is relational: human beings are made persons by the respect granted to their freedom by other human beings, not by that freedom itself. While this differs semantically from the notion of personhood developed through existential thought, it results in largely the same effect: that

\textsuperscript{512} Kant, supra note 490 at 30. \textsuperscript{513} Ibid at 30-31. \textsuperscript{514} Ibid at 31. \textsuperscript{515} Ibid at 30. \textsuperscript{516} Ibid at 160-161. \textsuperscript{517} Ibid at 30-31. \textsuperscript{518} Ibid at 186. \textsuperscript{519} Ibid.
personhood can be increased or decreased by the actions of others to limit personal freedom. Despite this possible extrapolation of Kantian philosophy to personhood, I proceed through the remainder of this Chapter using the notion of personhood previously developed with respect to existentialist thought.

By taking this view of personhood, legal protections for freedom of expression, anonymity, and privacy can be understood. Indeed, freedom of expression and privacy have often been associated with personal autonomy, identity, and self-development.\(^{520}\) As discussed in Chapter 2, these interests are central to the ability of individuals to self-develop their identities, choose their own purposes, and act upon those purposes. It will come as no surprise that some existential thought expressly refers to the construction of identities through life-narratives and stories,\(^{521}\) similar to the views of Professor Gaia Bernstein\(^{522}\) also discussed in Chapter 2. According to Charles Guignon, it may be that there is “no “real self” that exists below the stitched-together roles, projects, and identities that constitute [one’s] life story”.\(^{523}\) Thus, a person is an entity which is capable of defining itself and writing its own narrative, and personhood is the condition of being both free and able to do so.

Personhood in this conception is not binary; it is not something one simply has or does not have. It is something that can be expanded or contracted, enabled or restricted. It is the freedom to explore and choose one’s purpose, and to pursue it. This may sound like a definition of autonomy, but it is more than the legal or Kantian sense of autonomy, which envisions the freedom of the will to legislate universally for the self without being subjected to the coercion of others.\(^{524}\) This sense of autonomy is part of personhood, but unlike that notion of autonomy, personhood is something that can be expanded by advances in technology and knowledge. A person with the means to travel the world has more freedom than one trapped in his city of birth, even if that person never chooses to exercise that freedom. His freedom to intend and give


\(^{521}\) Aho, supra note 497 at 56-57.

\(^{522}\) Bernstein, supra note 8.


meaning has grown by virtue of the increase in possibilities and available knowledge. Thus, personhood can also be limited by the objective realities one confronts.

With this definition of personhood, we can also better understand the nature of harms to personhood. A harm to personhood is any action by another party that interferes with an individual’s freedom to choose one’s own identity and purposes, and to follow through on those purposes. We can see that limitations upon, for example, freedom of expression would do so by limiting both the ability of the person to receive information to choose her meanings and purposes, and the ability to speak in order to achieve the ends she sets for herself. Invasions of privacy and breaches of anonymity likewise destroy the self-defining essence of personhood by undermining the individual’s ability to control the roles they assume and masks they wear, as well as denying them the time and space necessary to reflect and order their thoughts so as to make considered choices as to their purposes.

I note that one of the possible problems of framing personhood in the existentialist or Kantian tradition—even to the limited extent I do here—is that these modes of thought are intrinsically individualistic, and is, in a sense, a denial of communitarian influence on identity. Indeed, some see existentialism as a school of thought that arose as a result of European societal changes that pulled people away from the traditional communitarian roles of medieval society into the modern individualistic state: a trend that reached its zenith during the industrial revolution. Whether or not this is true, it remains clear that my conception of personhood, is profoundly individualistic. My view does not outright reject the possibility of a communitarian identity or life narrative, but it does require that that identity was freely chosen by the individual, rather than adopted as a result of coercion. What constitutes coercion within the world of highly complex social structures and norms in which we live is open to debate, but so long as one sincerely chooses a communitarian identity, they’ve exercised their personhood. Thus communitarianism can still be a result of individualism.

One other concern is that this conception of personhood may appear to envision an idealized mental state, in which individuals are fully rational and capable of thoughtfully choosing from amongst all of the available options open to them. It thus may appear to gloss over psychological

\[525\] Aho, supra note 497 at 7.
realities such as subconscious thought and action, instinctual behaviour, decision-making heuristics, bounded rationality, and the result of mental illnesses or trauma. However, consideration of these factors is not inconsistent with my articulation of personhood and freedom. While some existentialist thought may suggest that hiding behind one’s passions or deterministic notions of individual action is acting in “bad faith,” and is therefore an error, in my view we can limit the scope of meaningful choice to that choice that is subject to free will. A perhaps intuitive view of the mind, and one that accords with the view largely taken by the legal system, is that the mind is neither fully deterministic nor fully subject to free will. While such a view is open to debate, we can assume that personhood operates to the extent that the law recognizes both the ability of individuals to choose for themselves and the inherent limits upon that ability.

3. The Internet for Personhood

To a certain extent, many, if not most, technologies affect individual freedom. Technologies typically allow people to do things they wouldn’t have been able to do without access to that technology, or at very least do things in different ways. Otherwise, a technology is often little practical utility. Thus, if we take personhood as consisting of the freedom to intend and pursue those intentions, perhaps the entire universe of technologies is expansive of personhood. We might then reach the conclusion that even minor differences in access to technologies, or the skills to use them, make some individuals more or less ‘people’ than others. However, this forgets the definitions established above. To reiterate, a person is an entity capable of defining itself and writing its own narrative. Personhood, by contrast, is the condition of being both free and able to do so. So two individuals are both people so long as they are capable of self-definition, regardless of any differences in freedoms or access to technology between them. But their condition of personhood may be different.

526 Sartre, supra note 493 at 47-49
527 For example, the criminal law generally holds people accountable for their actions but allows for certain exceptions where the evidence suggests the individual was not in control. Mental disorders are one defence to criminal culpability: Criminal Code, supra note 44, s 16(1). Automatism, such as sleepwalking, has also been recognized by the Supreme Court of Canada as a defence even in cases of murder: R v Parks, [1992] 2 SCR 871.
528 See e.g. Ruth Weintraub, “Psychological Determinism and Rationality” (1995) 43:1 Erkenntnis (1975-) 67 (discussing and critiquing various theories of rationality and determinism).
The above statement may seem jarring, that one’s personhood can be strengthened or lessened by exterior factors such as the existence of some technology. This is certainly true with respect to technologies that have a limited impact upon our abilities as people to write our own life stories and define ourselves. The invention of the umbrella hat\textsuperscript{529} is unlikely to have meaningfully affected the personhood of many people. Nonetheless, the problem of all technologies having some effect on personhood is a serious one, and one that must be investigated. Otherwise, a theory of legal adaptation to the Internet that focuses on its impacts upon personhood would be trivial if such considerations applied equally to all other technologies.

To begin this investigation, it’s important to distinguish between two general ways in which a technology might affect personhood. The first category is a relationship in which the effect on personhood is extrinsic to the technology itself, and the technology merely creates the nexus for some form of self-identification. Members of various professions or enthusiast groups, for example, may self-identify strongly in relation to a particular technology. For example, we can predict that both auto mechanics and classic car collectors may form some part of their conception of self around the technology of the automobile. However, the effects of such a relationship between the technology and individual personhood are limited insofar as nothing inherent in the technology gives rise to this relationship. Anything else could equally stand in for the automobile in this example.\textsuperscript{530} Instead, the effect on personhood is based solely upon individual preferences and attachments. People are likely capable of forming concepts of self in relation to any ideology, person, group, activity, technology or object. A person could, after all, identify strongly with the umbrella hat in the same way. Professor Margaret Jane Radin noted a similar concern in her seminal article on the relationship between personhood and property.\textsuperscript{531}

\textsuperscript{529} The umbrella hat is typically a small umbrella attached to a headband one puts on their head to allow for hands-free protection against the sun or rain.

\textsuperscript{530} Using the example of the automobile here may be confusing, since it could well be argued that it also has an intrinsic effect upon the personhood of its users by increasing their freedom of mobility. However, I use it only as an example of a technology to which people may attach part of their self-conception in the same way as they could with any other technology, or any other thing. Technologies can thus easily fall into either category, depending on the nature of the relationship between the person and the technology. I leave out a discussion of its inherently personhood-expanding aspects.

\textsuperscript{531} Note that I take a somewhat different view of personhood than Professor Radin, as we follow different philosophical traditions to reach the definition. Professor Radin’s view follows a line of reasoning from Hegel and Kant to posit that some property is constitutive of personhood insofar as people, to be people, need to exert some control over external resources. Property can thus be property for personhood where it is enabling of personal autonomy or closely tied to one’s self-development. While this is somewhat similar to my own definition, in her view, where property was closely tied to personhood, that property was better viewed as inalienable. While I do not
She argued that if we merely take property to be constitutive of personhood on the basis of individual subjective preferences and attachments, then we are doing little more than a “utilitarian preference summing.” There is then little reason to privilege these subjective preferences over any others by way of legal recognition. The same problem applies here. We therefore need some sort of criteria to determine what relationships between personhood and technologies are worthy of legal recognition.

This brings us to the second category of relationship between technologies and people, in which the technology has an inherent effect upon the personhood of its users as a result of the effects of its use. In my view, this is the category deserving of legal recognition, as its personhood impacts are not limited to those who simply choose to attach their conceptions of self to it, and its impact goes beyond subjective preference summing. This category includes many of the most impactful technological advances. The invention of written language is one example. The ability to preserve knowledge, communicate over distances and time, learn from history, and immortalize a part of the self is intrinsically expansive of personhood. The freedom to self-define, form an identity, and pursue one’s ends is expanded through the technology regardless of whether one strongly identifies with the written word. Additionally, we might also say that technologies that improve individual health are personhood expanding in the straightforward sense that they allow individuals to be free from physical limitations that restrict the ability to intend and act freely, up to and including death. However, it would be rare that we would need to address these technologies within a personhood framework, simply because their benefits are extremely socially well-recognized and respected, and individual morality tends to converge on the issue of physical health. There is thus little debate. Other technologies that have inherent personhood impacts might be more restricted in scope, and may only impact a limited group of people. For example, sex reassignment surgery directly affects personhood by enabling certain people to live

---

disagree that some property may be better treated as inalienable, my view of the connection between personhood and property would also support totally fungible property rights as promoting personhood as a way by which to better direct oneself towards one’s chosen purposes. See generally Radin, supra note 441.

532 Ibid at 961.

533 Again, we might expect authors, booksellers, editors, and many readers to self-identify closely in some way with written language. However, such a relationship would still fall in the first category, as this is a matter of subjective preferences and attachments, and is not inherent to written language itself.
their lives in a body more accurately depicting their conceptions of themselves. However, the procedure does not directly impact the lives of the vast majority of people.

It’s important to note that all technologies can give rise to relationships in the first category, as it’s based solely upon personal preferences, but only some are likely to give rise to strong relationships in the second category. Thus, we can differentiate technologies and their relationships to personhood on the simple basis of whether the technology inherently affects personhood, or whether any effect is merely a result of personal preferences and subjective attachments. However, this still does not get us past the problem, identified earlier, that most technologies are, in a sense, inherently personhood expanding for the simple reason that they allow for new possibilities and therefore new dimensions of freedom. Even the umbrella hat could be considered inherently personhood expanding in that it does, after all, allow one’s hands to be free to do other things while still being protected from the rain or sun outdoors. To the extent this increases the capacity for one to intend and pursue those intentions, this might be considered personhood expanding, even if in only a very limited sense. If we’re to view certain technologies as implicating personhood interests in such a way as to warrant legal recognition, then some line needs to be drawn on the issue of at what point a technology is sufficiently inherently personhood expanding to warrant such recognition. Such a line could well be drawn on a case-by-case analysis, especially as other factors may also be relevant. For example, we must also consider the number of people impacted. One technology may deeply impact the personhood interests of a small group of people, while another may marginally impact the personhood interests of a wide swath of the population. There is no a priori reason to prefer one or the other, or to set the bar at any particular point.

However, some objective criteria can be set by looking to whether interests already well established by the law and widely considered constitutive of personhood are affected or challenged by a technology. Where use of a technology inherently implicates well-recognized personhood interests, there can be a presumption that the technology may be sufficiently deserving of legal attention by virtue of its impact upon legal rights already recognized. While not completely determinative, this at least assists in making an assessment of which technologies might warrant special attention when addressing the ways in which they challenge existing law. However, making a judgment call on the degree to which personhood interests are impacted by a
technology may still be necessary, even with consideration of the factors discussed here. This is certainly something the law often does.\(^{534}\)

This brings us to our discussion of the Internet. My intention in this thesis was not to develop a theory that applied to all technologies broadly, but rather to create a substantive theory of legal adaptation to the Internet in particular. Therefore, while it may be important in future cases to consider the personhood implications of other technologies based upon the above discussion, here we need do so only with the Internet.

And in that respect, in my view, the analysis is clear. As was discussed at length in Chapter 2, the effects of the Internet on personhood are both broad in the scope of its user base and deep in respect of the manifold ways it has proved to be expansive of personhood. This is evidenced in its effects upon existing legal rights, and the manner in which it has pushed courts and lawmakers to address new problems, and to expand both the scope and protections of existing legal rights.

I’ve previously called these expansions of rights the creation of “digital rights.” By this, I mean only that rights such as freedom of expression, the right to anonymity, and the right to be free from interference within our personal domains must be understood in a broader sense within the Internet context, taking into account the ways in which the Internet is expansive of the underlying interests in those rights. Thus, these rights take on a new quality deserving of legal recognition in the online context. This does not necessarily mean that these rights are more deserving of protections in all cases, but rather that additional weight may need to be given to them when balanced against other interests. Anonymity, then, is a “digital right” with respect to Internet use insofar as the various protections for anonymity created by the courts apply uniquely within that context.\(^{535}\) Expansions to user rights under the Canadian Copyright Act\(^{536}\) that directly contemplate Internet use are similarly “digital rights,” such as the non-commercial user

\(^{534}\) Judicial decisions, perhaps especially in Canada, are rife with tests requiring the balancing of different qualitatively-determined factors in each case. For example, the current test for fair dealing under copyright law in Canada requires an analysis of six qualitative factors: *CCH Canadian Ltd v Law Society of Upper Canada, supra* note 224. The test for determining the appropriate procedural fairness requirements in administrative decision-making contexts was similarly determined by the Supreme Court of Canada to require consideration of five qualitatively-determined factors: *Baker v Canada (Minister of Citizenship and Immigration)*, [1999] 2 SCR 817.

\(^{535}\) See e.g. *R v Spencer, supra* note 140.

\(^{536}\) *Copyright Act, supra* note 213.
generated content exception.537 And protections for spam538 are clearly “digital rights” insofar as they almost exclusively apply to online communication. The manner in which this has already been done was discussed in Chapter 2, and I expand on some additional implications of this later in this Chapter.

What, then, is the substantive theory of legal adaptation that this thesis set out to develop? After much discussion, I hope to put it thusly: based upon past legal adaptations and challenges, we can observe that the Internet is a technology that expands personhood by offering new freedoms to self-develop and self-define. It does this by offering an enormous increase in users’ abilities to find the information necessary to make choices, to explore and define aspects of the self, to choose one’s purposes and ends, and to pursue those ends with sincerity. It is more than merely a communication tool, and an internal view must be taken to understand its human impact. Just as Professor Radin argued that property in the external world could be constitutive of personhood because of property’s function in self-identification and autonomy,539 so too can one’s Internet presence be constitutive of personhood in its power to expand those same interests. Personhood on the Internet encompasses the exploration and formation of identities, the expanded ability to speak or find the information one is looking for, the freedom to join and participate with communities at any level of anonymity, and the ability to engage with the world in deeply interactive and creative ways. It is also the scope for all of this to be abused to attack the essence of an individual’s sense of self. We are, in part, our digital selves, and thus we can speak of an “Internet personhood.” From a legal perspective, the implication of Internet personhood is straightforward: where legal adaptation to the Internet is under review, we must not only consider the way the affected rights have been traditionally construed, but also the way in which the digital environment has modified their importance with respect to personhood. Ultimately, this means that law makers should consider how a given policy choice or decision will increase or limit the freedom of individuals to self-determine and self-define.

537 Ibid, s 29.21. I note that this does not relate solely to content online, but its express inclusion in the Copyright Act is primarily aimed at Internet activity. See Hebb, supra note 230.
538 See e.g. CASL, supra note 60.
539 Radin, supra note 441.
Such determinations may not always be clear, even with respect to personhood. Indeed, in many cases, personhood interests may conflict, as freedom of expression and privacy often do.\textsuperscript{540} Of course, there is nothing new about similar conflicts of rights in the law. Canadian Charter jurisprudence, for example, is full of rights-balancing.\textsuperscript{541} The theory of Internet personhood offered here would add only that the impact of the Internet on the underlying personhood interests on each of the parties be taken into account within the rights balancing consideration. Examples of this are discussed in Part 4, below.

A theory of Internet personhood also allows us to better understand how the denial of the personhood expanding aspects of the Internet might result in harms. To destroy one’s anonymity through an unwanted disclosure of identifying information can be seen as a harm, as it undermines the ability of an individual to control their identity and to freely pursue their ends without outside influence.\textsuperscript{542} Supressing freedom of expression on the Internet by the over-application of copyright law or defamation law is similarly a harm insofar as it suppresses the ability of individuals to both pursue their ends and the ability to receive information critical to self-development and the creation of meaning and purpose.\textsuperscript{543} The intrusion into the personal digital domain, such as through the abuse of spam, is a harm by virtue of its power to repress individual autonomy.\textsuperscript{544}

One might contend that there is no harm in preventing the ability of individuals to make use of the expanded opportunities for identity formation, self-development, and expression on the Internet. The Internet has not always existed, and individuals were not held to be in a state of constant harm by being deprived of some advantage provided by a future technology. Under this view, the Internet is a technological privilege, and no harm can be said to arise from the denial of

\textsuperscript{540} One prominent international example is the case of \textit{Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González} (13 May 2014) C-131/12 (CJEU), online: EUR-Lex <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:62012CJ013>. In that case, the Court of Justice of the European Union required Google to remove links to content concerning individuals who requested that it be removed under the EU “right to be forgotten”. The case put privacy and freedom of expression in direct conflict.

\textsuperscript{541} See e.g. \textit{R v NS}, 2012 SCC 72, [2012] 3 SCR 726 (in which the Supreme Court had to balance the accused’s right to a fair trial against a witness’ right to freedom of religion resulting from the latter’s request to wear a niqab while testifying); \textit{Dagenais v Canadian Broadcasting Corp.}, [1994] 3 SCR 835 (in which the Supreme Court had to balance the accused’s right to a fair trial against the media’s right to freedom of expression with respect to a publication ban).

\textsuperscript{542} See Chapter 2, Part 4(a), \textit{supra}.

\textsuperscript{543} See Chapter 2, Part 4(b), \textit{supra}.

\textsuperscript{544} See Chapter 2, Part 4(c), \textit{supra}.
a privilege. Even if it does expand the personhood interests of its users, it still cannot be a harm to deny access to those benefits because it can’t be a harm to take away what was only just granted.

However, this argument must fail. While it may be true that the denial of a privilege is not a harm, the decision as to what is and what is not a privilege becomes determinative of the issue. For example, we do not consider the ownership of property a privilege, and thus the law holds it to be a harm should a person be deprived of their personal property. However, we could imagine a universe in which the law does not respect notions of property beyond, say, that immediately necessary for life, and considers any additional property possession a mere privilege freely revoked. However, as a society, we’ve decided that the benefits of a right to property ownership are great enough to warrant legal protection. Therefore, property is a right and not a privilege. Similar conclusions can be made about other technologies, such as medical technologies, water purification technologies, or even electricity generation. We would generally consider, I think, the denial of medical care, clean water, or electricity to a person to be a harm, even if people once lived without access to those things and were not considered to be living in a state of harm. Based upon the personhood considerations described above and the adaptations made by the courts and legislatures with respect to the Internet, in my view, seeing the personhood expanding aspects of the Internet as a right rather than a privilege is the preferable view. Indeed, as will be discussed below in Part 4(d), there is also a growing consensus that the Internet is more than merely a privilege or a luxury, and is instead something that people can expect to reasonably rely upon and enjoy without interference.

Before we begin exploring the implications of Internet personhood, it is important to note that personhood will not always be applicable to all legal adaptations to the Internet. Many of the areas of legal adaptation to the Internet discussed in Part 2 of the previous Chapter may remain unaffected by personhood considerations. Some adaptations may merely apply the law to the Internet in prosaic ways. Legislative attempts to ensure that electronic agreements are enforceable are also unlikely to deeply involve personhood interests. However, in my view, the theory is applicable to a number of potential areas of future concern. I now turn to a

545 See e.g. Criminal Code, supra note 44, s 322 (regarding theft).
546 See e.g. Electronic Commerce Act, supra note 205.
consideration to the implications of personhood as a substantive theory of legal adaptation to the Internet.

4. Implications of Personhood on the Internet
   a. Anonymity Protections

In Chapter 2, I discussed anonymity and pseudonymity at some length with respect to recent judicial decisions concerning the identification of Internet users in cases of copyright infringement and defamation, as well as for criminal prosecution. Here, however, I want to discuss Internet anonymity as a fundamental principle of Internet regulation.

Bryan H Choi has argued that there is a tension between the Internet’s “generativity” and its anonymity.\textsuperscript{547} Here, “generativity” is a term coined by Professor Jonathan Zittrain to refer to “a system's capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences.”\textsuperscript{548} The basis of the argument is a descriptive one: that generativity, which is the spontaneous and unexpected innovation observable on the Internet, also provides a broad scope for abuse.\textsuperscript{549} If we want to address these abuses, such as copyright infringement,\textsuperscript{550} access by children to adult content,\textsuperscript{551} and defamation,\textsuperscript{552} he argues that one way is by regulating anonymity.\textsuperscript{553} Generativity, he argues, is of more social importance, and thus it is anonymity that must give way where the two come into conflict.\textsuperscript{554}

We can see this conflict between generativity and anonymity in the issue of anonymous defamation. If we’re concerned about limiting defamation, then we can either choose to allow for a process of reasonable identification of defamers, and thus limiting anonymity, or we can institute regulations that might put increased responsibility on publishers, website hosts and other intermediaries to regulate their content. Taking the latter approach would limit generativity by having a chilling effect on the creation and operation of intermediary services open to user-

\textsuperscript{547} Choi, supra note 14.
\textsuperscript{548} Jonathan Zittrain, \textit{The Future of the Internet—And How to Stop It} (Yale University Press, 2008) at 53.
\textsuperscript{549} Choi, supra note 14 at 504-506.
\textsuperscript{550} Ibid at 508-516.
\textsuperscript{551} Ibid at 508-523.
\textsuperscript{552} Ibid at 529-523.
\textsuperscript{553} Ibid at 506.
\textsuperscript{554} Ibid.
generated content, as the costs to these intermediary services of either moderating the content or fighting resulting lawsuits might be prohibitive. While Choi brings up other possible abuses, defamation is only area that is persuasively a continuing problem on the Internet. Indeed, copyright owners are increasingly finding ways to monetize their infringed content, such as through YouTube’s Content ID system, in ways that attempt to sacrifice neither anonymity nor generativity, while copyright laws are, in some cases, moving to open up more avenues for Internet generativity at the expense of copyright. We are, therefore, increasingly finding that limiting anonymity or generativity is unnecessary with respect to intellectual property, and it can be argued that protecting intellectual property inherently undermines generativity. The same is true with respect to children’s access to adult materials, which from the lack of recent political debate or criminal prosecutions regarding access to otherwise legal pornography, we appear to have simply decided it isn’t that important an issue to begin with. And while Choi mentions spam, he notes that the route taken to address it is already one that goes after spammers on an identity basis rather than a generativity basis.

Thus only defamation remains to bolster the descriptive argument. Defamation is a real cause for concern, and one’s right to their reputation is perhaps equally a personhood right. As identity is largely a matter of controlling the perceptions of one’s audience, reputation is clearly partly constitutive of identity, and thus of personhood. Thus we have two personhood rights in conflict. The danger here is to underappreciate the benefits of anonymity, as Choi does by limiting its benefits to the ability to “resist authoritarian control” and to promote freedom of expression. The analysis must be deeper. Because of the importance of anonymity to a great deal of Internet activity, we must be prepared to face generative consequences of a lack of anonymity. Anonymity is enabling of speech that otherwise might be restricted or chilled. Thus, we must

555 Ibid.
556 YouTube allows copyright holders in songs to redirect all ad revenue from a YouTube video to that rights-holder if the Content ID system detects the use of a copyrighted song. See Benjamin Boroughf, “The Next Great YouTube: Improving Content ID to Foster Creativity, Cooperation, and Fair Compensation” (2015) 25 Alb LJ Sci & Tech 95.
557 See Chapter 2, Part 4(b), supra.
558 See e.g. Carrier, supra note 3 (arguing that modern copyright law can impede innovation rather than promote it).
560 Choi, supra note 14 at 524.
561 See e.g. Westin, supra note 239 at 31-32; Austin, “Anonymous Blogging”, supra note 140.
562 Choi, supra note 14 at 541.
563 Ibid at 549.
564 Ibid at 549.
ask whether we would have the same creativity present on YouTube, Soundcloud, DeviantArt and many other platforms featuring user-generated content if the creators of those works were readily identifiable, and thus able to be sued, by copyright owners? Would the new non-commercial user generated content exception, which was likely spurred by the stunning displays of personal expression in remixes and mashups, exist?

Further, we need to balance the underlying interests at stake on each side of the issue. This is where the present theory can offer some guidance. Reputation is important. So too is anonymity. But it’s critical to understand why these sets of rights are important in order to reach a proper balance. If anonymity is only important because it allows for political speech that might otherwise be repressed in a totalitarian state, then anonymous speech concerning private citizens or containing aesthetic messages warrants no protection. However, if we understand anonymity on the Internet as central to one’s ability to obtain information, control one’s identity, explore aspects of the self, and pursue one’s ends without being held to comply with extant social norms and face the debilitation of constant surveillance, then we view anonymity as deserving of protection with respect to all speech online. Reputation is of similar importance, being critical to one’s sense of self, identity, and psychological health. It’s not clear that one should be privileged over the other. Indeed, the summary judgment standard, or requirement to show a prima facie defamation case, used by many courts is one possible balancing of these issues that neither discards anonymity nor gives a free pass to online defamers. I leave a discussion of whether or not this is the proper balancing for a future discussion.

Nonetheless, the issue illustrates the importance of not missing the underlying importance of digital rights. The courts have not expanded these rights in the Internet context without reason, even if that reason has proven difficult to articulate. Limiting anonymity can, in some scenarios, be one lever by which we can respect rights such as reputation without directly damaging the generativity of the Internet. But before that lever is pulled, a careful consideration of both how

---

565 Hebb, supra note 230 at 238.
567 See e.g. Warman v Wilkins-Fournier, supra note 265; Doe No 1 v Cahill, supra note 277.
undermining anonymity also undermines generativity, and how weak anonymity undermines the
very value of the Internet to a large number of its users.

Taking the argument in a slightly different direction, we can also see how considerations of the
importance of Internet personhood might shape future rights balancing. Consider the case in
which one Internet user wishes to divulge the real name of another anonymous Internet user
against that user’s wishes. This is often referred to on the Internet as “doxing,” and can be used
as a method to coerce, intimidate or punish other Internet users.\footnote{Doxing is sometimes also spelled “doxxing.” C S-W, “What doxxing is, and why it matters,” The Economist (20
March 2014) online: <http://www.economist.com/blogs/economist-explains/2014/03/economist-explains-9>.} It may, as well, be used with
less injurious intentions, such as to reveal that an anonymous speaker may have ulterior motives
for their comments. In either case, however, the first party’s interest in freedom of expression
comes into direct conflict with the second person’s interest in anonymity. While it’s unclear
what, if any, laws apply directly to a doxing scenario, at least where the identifying information
was obtained through legal channels such as personal knowledge or public records and the use
does not amount to harassment, considerations of the personhood interests may well support a
cause of action. Most of the same concerns about identifying anonymous Internet users discussed
in Part 4(a) of Chapter 2 apply here as well. Naturally, the issue of how to prohibit abusive cases
of doxing while allowing for doxing that may prove to be in the public interest would remain a
problem. As the interaction between freedom of expression and privacy interests are complex, I
leave a more fulsome argument concerning the issue to a later date.

b. Virtual Property

Virtual property is property that only exists within virtual worlds such as video games and other
virtual realities. Professor Joshua Fairfield has defined virtual property as “[r]ivalrous,
property may be a house in the virtual world of Second Life, or a powerful sword in the game of
World of Warcraft. Virtual property has significant economic value. Ten years ago, the estimated
trade value of virtual property was in the billions of dollars, and it’s likely to have continued to
Some individuals have become real world millionaires through the acquisition of virtual property. As virtual property exhibits a number of the hallmarks of real property, such as rivalry, persistence, and transferability, it stands to reason that some “owners” of virtual property would begin to assert legal rights in it. Indeed, various courts and regulators around the world have already suggested that virtual property will be treated as property in some contexts. In China, a video game player successfully sued a game developer for failing to protect his virtual property from theft. In the Netherlands, a man was convicted of theft for stealing a virtual amulet. And in Taiwan, the legislatures have recognized virtual property as property under the Taiwanese Criminal Code.

A number of commentators have already discussed the possibilities of applying real-world property law to virtual property interests, under both economic and Lockean labour theories. Much of the current debate surrounding property rights in virtual property concerns the contractual relationship between the developer and users, usually embodied in an End User License Agreement, and whether a property rights regime could or should override that contractual relationship.

---

572 See Fairfield, “Virtual Property”, supra note 15 (discussing the similarities between real and virtual property at 1053-54).
577 For examples of the debate on the applicability of End User License Agreements to virtual property, see Jamie J Kayser, “New New-World: Virtual Property and the End User License Agreement” (2006-2007) 27 Loy LA Ent LR 61; Lawrence, supra note 15; and Fairfield, ibid.
A theory of personhood on the Internet is germane to the debate. If personhood is partially constituted in the online space, it gives credence to the notion that property rights in virtual goods may themselves be an extension of personhood interests. If we can have personhood interests in our online presence, as this thesis has argued, and if we can have personhood interests in property, as Professor Radin has argued, it stands to reason that personhood interests might map onto virtual property. Indeed, this has already been suggested by at least one commentator.579

This argument deserves some further explanation. We begin with observation, argued at length in this thesis, that individuals have personhood interests in their online presence. Virtual property most commonly exists within virtual worlds such as video games, in which players take on the roles of one or more characters, often known as “avatars.”580 These avatars can be seen as a form of pseudonym, or alternate identity. As discussed, pseudonymous identities can be constitutive of self by allowing individuals to operate outside of the traditional social norms that govern their behaviour, and to explore aspects of self that might otherwise be repressed.581 But if these identities are to truly be valued as constitutive of personhood, they themselves must be capable of allowing an individual to explore the implications of that identity. If one takes on pseudonym but cannot speak or act under that pseudonym, the pseudonym loses its value. Each way in which that pseudonymous identity can be used furthers its usefulness in self-exploration and determination. An author whose friends call him by his pseudonym but whose publisher refuses to publish his book under it gains less utility from that pseudonym than one whose publisher will use it. And virtual worlds are an extremely powerful use of a pseudonymous identity. They attempt, in many ways, to recreate real spaces, real social interactions, and often real economies that players all interact with under alternate identities.582 They therefore offer perhaps the most complete opportunity to truly inhabit an alternate identity while still engaging in much of the same conduct as people in the real world. Property, insofar as it relates to personhood, can thus be construed as one use of an identity. For one to fully inhabit an alternate identity and gain its benefits, that identity, like the real world identity of the person, may be expanded by the

578 Radin, supra note 441.
581 See Chapter 2, Part 4(a) supra.
582 Boone, supra note 579 at 718-720.
recognition of property rights to virtual property. Thus, property rights in virtual property may
make the use of alternate identities even more useful to explore the socially repressed aspects of
self that pseudonyms are capable of, and thus to better self-define and self-determine.

This explanation is somewhat problematic, however. It requires the assumption of a two stage
connection between the property and the person. The first connection is between the person and
their avatar identity, and the second is between the avatar identity and the property. If either
connection is weak, then the personhood justification for property rights is undermined. Indeed,
while there are surely many players that closely identify with their avatars and whose avatars
constitute an important part of their self-conception, we would likely assume that for the vast
majority of players this is not the case.

A virtual property for personhood rationale could rest on a more direct connection between the
player and the virtual property. Here, the argument goes that the intermediary avatar is simply an
extension of the player’s real identity into the virtual world, and that the virtual property
“owned” by that avatar is really just the property of the player. Thus, the personhood in the
virtual property is a more direct application of Professor Radin’s views on the relationship
between property and personhood.583 This is certainly the more intuitive argument, and the one
advanced by Professor Boone in his article on the subject.584 As Boone notes, however, a major
problem of attempting to apply Radin’s personhood theory to virtual property is that it militates
towards the inalienability of the property rather than its free trade.585 Indeed, the primary
implication of Radin’s discussion of the relationship between property and personhood was to
put property on a spectrum between fungible and personal.586 As Boone notes, the recognition of
strong “personal” property interests in virtual property would defeat much of the purpose for
which property interests in virtual property have been called for in the first place by undermining
the importance of alienability and trade.587

Here, however, the differences between Radin’s view of personhood and my own are relevant.
Radin talks of the personhood relationship between persons and property as primarily based in

583 Radin, supra note 441.
584 Boone, supra note 579.
585 Ibid at 742.
586 Radin, supra note 441 at 986.
587 Boone, supra note 579 at 742-743.
the notion that particular pieces of property become “bound up” with the self. Thus, a wedding ring may be fungible to the jeweller selling it, but deeply personal to the women who eventually wears it. Radin suggests that “[o]ne may gauge the strength or significance of someone's relationship with an object by the kind of pain that would be occasioned by its loss.” We can thus see Radin’s view of property for personhood as based upon particular subjective relationships between individuals and objects. Her theory does not, therefore, extend to justify all property rights, whether fungible or personal, but rather focuses on justifying the potential inalienability of the latter.

My own view of personhood is consistent with Radin’s view, but somewhat broader. Indeed, one’s close subjective relationship with an object may implicate personhood insofar as it forms the basis of one’s conception of identity and one’s creation of meaning and purpose. This is similar to the discussion in Part 3, above, of how one’s identification with a particular technology may be expansive of personhood. Radin moves past the problem of this being a subjective “utilitarian preference summing” by attempting to differentiate those kinds of property attachments that are healthy from those that are fetishistic. However, it can be recalled I moved past this similar problem with respect to technological attachment by avoiding such inherently subjective relations altogether and looking to find what it is inherent in the relationship between the technology and the person (e.g. the common use of the technology) that is expansive of personhood.

With respect to property, the same can be done by viewing the institution of property generally as expansive of personhood, rather than looking to individual-object relations. Each right in the bundle of rights commonly viewed as making up what we call “property” grants the holder the ability to deal with an external resource in a way that increases her ability to choose and pursue

588 Radin, supra note 441 at 968.
589 Ibid at 959, 987-988.
590 Ibid at 959.
591 Ibid at 961.
592 Ibid at 962-970.
593 I do not argue that such subjective relations are unimportant. Indeed, they may well militate for certain property rights to be inalienable, although I believe that such a utilitarian preference summing or economic analysis may be the proper way to demonstrate this. However, in my view, without more they form an unpersuasive basis for the legal recognition of additional rights.
594 See Chapter 3, Part 3, supra.
her own ends. For example, the right to exclude others from access to or using certain property ensures that an individual can make plans that rely on the exclusive future use of that property without entering into possibly onerous negotiations regarding that use. Most other rights, such as the right to subdivide, consume, or modify the subject of property also allow the property owner to make use of the property in way that allows the pursuit of her own ends without requiring the permission of others, and thus being beholden to them. In the same vein, the right to alienate, such as through trade or sale, is equally important to autonomy and personhood. If one is prevented from alienating property, they may be limited from pursuing one’s ends. As trade is generally viewed as a mutually beneficial transaction for the parties involved with each party gaining something of more value to them than the thing given, it stands to reason that personhood interests are increased by such transactions. The view of personhood presented in this thesis would see the subjective differences in valuation between the parties as arising from the differences in existential meaning and purpose taken by those parties. Thus, to exchange one resource of subjectively lesser value for another resource of subjectively greater value is inherently to pursue one’s ends; if it were not, the difference in subjective value between the exchanged resources would not exist. In that sense, the fact that virtual property has been exchanged for real money is evidence of personhood interests in virtual property.

This view is thus consonant with an economic view of property, but it also allows for much of Radin’s view of inalienability. It may be that the personhood implications of a given piece of property are so great as to make any kind of Pareto-optimal trade impossible. In such a case, any situation in which the property owner is forced to accept some externally-calculated market value in exchange for the loss of that property would be contractive of personhood.

With respect to virtual property, however, the personhood considerations suggest that a general standard property regime, which includes the right to alienate and transact, would generally be expansive of personhood and would allow the users of virtual worlds to both further explore aspects of self by more fully inhabiting their avatars and to pursue their own ends through the

---

597 The existence of any non-zero subjective valuation of an object is evidence of a personhood interest in that object, however weak. For this purpose, personhood can be seen as a species of utility.
598 This accords with Radin’s views on the subject of external appropriation, such as eminent domain: Radin, supra note 441 at 1005.
acquisition and disposition of virtual property. It would also roundly suggest that the theft of virtual property by other players should be treated in the same way as theft of property in the real world. As with an application of Radin’s analysis, it may be that some virtual property becomes fundamentally bound up with the self-identification of the user. Here, personhood interests would militate towards some protections from the arbitrary deletion, appropriation, or alteration of that virtual property by either other users or those who control the virtual world.

There are, of course, still a great many practical problems—a discussion of which is beyond the scope of this thesis—that would have to be addressed before any kind of virtual property rights regime could be implemented. The principal problem is that of the considerable control in the hands of the operator of the virtual world. If virtual property can be personal property, and if virtual property exists only upon the maintenance and consistency of Internet servers, one must find a balance between the competing personhood interests in the property and the interests of the operator in being able to modify or terminate the virtual environment in which the property exists.  

To address this problem, we could imagine a virtual property rights regime that governed relationships between individual users, but that was silent with respect to the operators of the virtual worlds. This would be one, albeit incomplete, solution. Another problem is the lack of well-recognized normative interests in virtual property, which undermines a common sense application of personhood to property. Nonetheless, if the significant disputes over virtual property are any indication, real interests can certainly be at stake, and an application of personhood considerations may be critical in ensuring that the proper balancing of interests is reached.

c. Anonymous Defamation

Many Internet users structure a considerable part of their lives around pseudonymous identities. These identities allow individuals to interact with others in ways that would not be possible in the real world, and to build reputations without attachment to their physical

---

599 For more in-depth considerations of this issue, see Fairfield, “Virtual Property”, supra note 15 at 1097-1100; Boone, supra note 579 at 737-741.
600 At least one murder has already been committed in a virtual property dispute: “Chinese gamer sentenced to life” BBC News (8 June 2005), online: <http://news.bbc.co.uk/2/hi/technology/4072704.stm>.
601 See generally Bernstein, supra note 8; Cole Stryker, Hacking the Future: Privacy, Identity, and Anonymity on the Web (New York: Overlook Duckworth, 2012).
Individuals may use these identities to write blogs, create videos, comment on the works of others, or participate in any number of communities or virtual worlds. Considerable time and effort may go into establishing oneself in the community and to gaining the trust of others. But if these reputations are undermined by defamatory statements, should there be a legal remedy?

The ability of plaintiffs to bring an action for defamation in respect of statements by anonymous Internet users has been well-explored in the academic literature and in the US courts. As discussed in Chapter 2, increasing protections for anonymity appear to be the norm in actions brought to reveal the identity of alleged tortfeasors, although such actions still often succeed where the claim appears meritorious. However, the inverse of this case—in which an Internet user brings an action in respect of a defamatory statement that identifies only the plaintiff’s pseudonym—has been little discussed.

Normally, a plaintiff in a defamation case must show that the words complained of referred to the plaintiff. Where the defamatory statement identifies the plaintiff only through a pseudonym, it appears that the plaintiff must establish that the public, or at least some members of the public, would be able to identify the true identity of plaintiff by reference to the pseudonym. In other words, the connection between the true identity of the plaintiff and pseudonym must be known by at least some members of the public. This was the case in Baglow v Smith, where the defamatory statement made by the defendant only referred to the

---

602 See e.g. Bernstein, *ibid* (discussing the case of a fifteen year old boy who built a reputation as a legal expert online at 984-986).


604 See e.g. *Doe v Cahill, supra* note 277; *Dendrite International Inc v Doe, supra* note 276; *Krinsky v Doe 6*, 159 Cal App (4th) 1154 (Cal Ct App 2008).

605 See Chapter 2, Part 4(b).


608 See e.g. *Foulidas v Ford*, 2014 ONCA 530, 242 ACWS (3d) 745 at paras 23-32.


610 *Baglow v Smith, ibid.*
pseudonym used by the plaintiff, ‘Dr. Dawg’.\textsuperscript{611} However, the Ontario Superior Court of Justice found that the plaintiff was sufficiently identifiable by his pseudonym as he had made no efforts to hide his true identity, and had previously used both his real name and pseudonym in conjunction within the same article.\textsuperscript{612} Thus, there was a connection in the minds of a sufficient number of members of the public between the pseudonym ‘Dr. Dawg’ and the plaintiff’s true name to assert that the impugned statement identified the plaintiff.

Considerations of Internet personhood, however, suggest that the law should potentially recognize a right to bring an action for defamation in respect of a pseudonym, even where that pseudonym cannot readily be tied to a real-world identity. If part of one’s personhood is partially constituted by pseudonymous identities, insofar as one’s sense of self has become bound up with these fragmented identities, then there is a real harm in having those pseudonymous identities defamed. For an individual whose sense and understanding of self is inextricably tied to one or more fragmented identities, having those identities become subject to public derision may be emotionally and psychologically harmful, and damaging to the invention of self and purpose that underlies personhood. Additionally, of course, such reputational damage could injure pecuniary interests if the identity was used for commercial purposes. For some, the harm may be equal to, or even exceed, the harm done by a similar defamation of their real identity. Where an online (or, indeed, offline) identity serves as a refuge from oppressive social norms in the real world, this may be doubly true. We might, then, predict that courts will be forced to consider the issue in future cases.

I note that I do not advocate that a right to one’s reputation in a pseudonymous identity should necessarily be recognized by the law, however. It may be that there are strong public policy interests in allowing the defamation of pseudonymous identities. The implementation may also be very problematic. The importance given to a pseudonymous identity can vary widely, and the courts may neither want to assume that all defamation of pseudonymous identities is harmful, nor engage in a detailed case-by-case analysis of the attachment of any person to their pseudonyms. Additionally, we might expect that pseudonymous plaintiffs would desire to keep

\textsuperscript{611} The impugned statement was the following: “Dr. Dawg's colourfully illustrated op-ed that describes the conservative base (for which nobody has claimed non-existence) amounts to "yokels with pitchforks." This coming from one of the Taliban's more vocal supporters.” \textit{Ibid} at para 11.

\textsuperscript{612} \textit{Ibid} at paras 172-174
their true identities secret, and so either would not bring suit, or would seek to bring suit under a mechanism that allowed them to remain pseudonymous. Whether the courts would be willing to allow for pseudonymous or anonymous litigants is another matter entirely, and I leave a discussion of that issue for another time.

d. Net Neutrality and the Internet as a Human Right

The questions of net neutrality and whether Internet access is a human right have received a great deal of academic and political attention recently. The two issues are distinct in their impacts upon individuals, but they are also related with respect to some of the arguments in favour of either. I do not purport to discuss either issue in depth, but merely to suggest that considerations of the impact of the Internet upon personhood are germane to both.

I turn first to net neutrality. Net neutrality refers to a policy that would require providers of Internet access to treat all communications in a non-discriminatory manner. Thus, those who control the transmission of data over the Internet would be required to ensure that certain types of data or data from certain sources aren’t treated preferentially over other data. In a practical sense, this means that broadband providers cannot, say, prioritize the data of their corporate partners over their corporate rivals or grant certain favoured web applications higher connection speeds than others. Proponents of network neutrality argue that a lack of net neutrality will stifle Internet innovation by allowing large existing content providers to effectively pay broadband providers to prioritize their data over those of new entrants with new platforms or applications.

While the debate surrounding net neutrality is broad and incorporates a large number of arguments and issues, a consideration of personhood interests also generally militates in favour of net neutrality regulation. If the fears are true that some data may be prioritized over other data should there not be net neutrality regulations, then it’s quite clear that personhood interests could be compromised should this happen. Where information, services or communities that may be expansive of personhood are blocked or restricted by Internet access providers,

---

613 See Skepys, supra note 126 (discussing the academic and political attention to the issue of the Internet as a human right at 15); French, supra note 13 (reviewing the net neutrality debate at 119-128).
614 Becker & Carlton, supra note 13 at 498.
616 French, supra note 13 at 122-123.
617 See generally ibid.
individuals who otherwise would benefit from an increased ability to self-define and self-determine will be negatively impacted through a limitation of that ability. We need not address this argument in any great detail, as its premises and logic should be by now self-evident. We can simply summarize it as follows: if the Internet is expansive of personhood by offering an increased freedom to self-define, create meaning, and self-determine, then limitations being placed on what can be accessed, communicated, and used on the Internet will almost certainly hinder that freedom.

A very recent decision of the United States Court of Appeals for the District of Columbia Circuit,618 which reviewed the Federal Communications Commission’s reclassification of the Internet as a “telecommunications service” for the purposes of net neutrality regulations, may have implied this in noting the importance of the third-party Internet content to the interests of Internet users:

Indeed, given the tremendous impact third-party internet content has had on our society, it would be hard to deny its dominance in the broadband experience. Over the past two decades, this content has transformed nearly every aspect of our lives, from profound actions like choosing a leader, building a career, and falling in love to more quotidian ones like hailing a cab and watching a movie.619

In saying this, the Court was dismissing objections that broadband access providers could be viewed as a complete content service rather than primarily a carrier of content created and distributed by third parties. Thus, the Court was asserting, broadband access providers are better seen as telecommunications services rather than content-creating and delivering information services. Given the profound effects of this third party content upon individual personhood, including those noted by the Court above, it’s clear that ensuring non-discrimination with respect to third-party content would be promoted by a consideration of personhood interests.

Many of the considerations might apply to the issue of viewing Internet access as a human right. The notion has already gained traction in Europe, with either courts or legislators in Estonia, Estonia, Finland, France, Greece and Spain all declaring Internet access to be a fundamental

---

619 Ibid at 26.
right. However, one of the problems with asserting that the Internet is a human right is the lack of consensus regarding what exactly defines human rights, and thus what qualities or status a human interest must have before it can qualify as a human right.

Much human rights scholarship views human rights as a form of natural rights that arise and attach to people simply by virtue of being human. The premise of these rights is that they’re engendered by some larger authority, whether that be God or the universe or some other higher reason. As should be clear from the forgoing discussion of existential thought, a theory of personhood based upon existential thought is unlikely to embrace a natural rights theory. Indeed, the maxim that “existence precedes essence” precludes viewing any rights as inherent in being human. Rather, it would assert the total lack of pre-existing rights or any higher authority on which to base such a theory of rights. In my view, this theory is more in line with what Professor Dembour refers to as the “deliberative school” of thought on the issue of human rights. Under this view, human rights are something that are created through negotiation, agreement, and consensus. Thus, human rights are something that are created by choice, which is more consistent with the approach taken in this thesis. Additionally, this view sees human rights as largely aspirational: they are moral claims that are held by their proponents to be universal, even if they are not universally respected.

While we can ground our view of human rights in this deliberative notion, this does little to answer the question of which rights should be universalized as human rights. After all, if we choose which rights to call human rights, there should presumably be some principled basis on which to identify human rights lest human rights debate devolve into a cacophony of claims motivated by individual interests. Fortunately, the personhood theory articulated here offers some assistance: those rights that are substantially necessary for the bulk of humanity to exercise the freedom to create meaning, self-define, choose one’s ends, and pursue those ends, could be those to which we attach the ‘human rights’ label. Naturally, determining which interests are

---

620 Skepys supra note 126 at 16.
622 Ibid.
623 Sartre, supra note 493 at 22.
624 Dembour, supra note 621 at 3.
625 Ibid.
sufficiently expansive of personhood to be worthy of being called human requires some arbitrary line-drawing that must be done by agreement and consensus. However, as we’ve seen, the Internet has been sufficiently expansive of personhood to warrant significant legal protections and thus might presumptively be considered a candidate for elevation to the status of a human or fundamental right.

As noted above, a number of European countries have begun to view Internet access as a human right, or at least an interest strongly implicating recognized human rights. For example, in France, the Constitutional Council held that Internet access was protected more generally under the right to “free communication of ideas and opinions” stating that:

> In the current state of the means of communication and given the generalized development of public online communication services and the importance of the latter for the participation in democracy and the expression of ideas and opinions, this right implies freedom to access such services.

Regardless of whether the debate concerns Internet access as a fundamental right by virtue of its implication of well-recognized human rights, or whether it concerns Internet access a human right of its own accord, some consideration of the personhood implications of the Internet are germane. As these personhood implications are indicative of the importance of the Internet to individuals both in its own right and with respect to other rights, such as freedom of expression, they serve to provide some principled basis on which to discuss the moral value of declaring Internet access a human right. As should be clear, the view taken in this thesis would conclude that these interests militate in strong legal protections for Internet access and use, and thus suggest a view of the Internet as at least a very important right implicating many existing rights, if not a human right. While I leave a more complete discussion of the Internet as a human right to another time, a deeper understanding of the personhood implications of Internet use can contribute to the debate and assist in the deliberative process of human rights formation by providing a reference point for the valuation of its importance.

---

627 Cons const, 10 June 2009, *Act furthering the diffusion and protection of creation on the Internet* (2009) JO 9675, 2009-580 DC at para 13 (referring to Article 11 of the *Declaration of the Rights of Man and the Citizen of 1789*).

628 Ibid.
Conclusion

This thesis has proceeded under three fundamental assumptions. The first is that the law does and should attempt to protect the interests, at least to some degree, of those to which it applies. The second is that the interests of people and society are not fixed, but change over time. The third is that technological change can motivate such alterations in interests.

If these assumptions are true, then the law must adapt to technological change. Even if the law were to be based upon the broadest standards and principles, rather than specific rules, we can expect that at some point, even those standards and principles might need revision. Of course, our law is not written nor adjudicated to promulgate the broadest of standards. And thus, as both technology and society’s relationship to it are always changing, the law must change with them.

How to change the law, however, is often a problem with few obvious answers. Changes to the law may have unforeseen effects, and it’s often impossible to know how a new technology has or will impact individual or group interests, especially early in its life cycle. As we’ve seen in Chapter 1, technology can impact the law in a large number of ways, and the possibilities for legal adaptation are as broad as the law itself.

In many cases, this is a problem with no ascertainable answers. We cannot expect good legal responses when there is a dearth of information about that which the law is trying to address. The best we can do is try to find ways to have as much information as possible when faced with a new technology.

Legal commentators can approach this problem in one of two ways. The first is to propose or modify existing procedural mechanisms so that new technologies can be reviewed and analyzed, and new laws researched and considered.\textsuperscript{629} We might appoint technological committees, empower administrative agencies, work with law reform committees to better adapt the law to the challenges of new technologies, or merely better identify the best decision-makers to handle legal adaptation to technological change. The second way is to look at specific technologies in order to discuss their general impacts and the way society, individuals, and—where applicable—

\textsuperscript{629} See e.g. Lyria Bennett Moses, “Agents of Change”, supra note 22.
the law, have responded to them. By doing so, these substantive theories attempt to understand a specific technology. Unfortunately, attempts to address legal responses to specific technologies in a way that moves beyond a focus on a specific doctrinal category are rare.

The promise of this thesis was to offer one such substantive theory with respect to the Internet and demonstrate its utility. As we’ve seen, this method looks at existing legal responses, endeavours to find commonalities in those responses, and then attempts to articulate a theory of the underlying rationale that motivates those responses even if that rationale could not be articulated by the decision-makers at the time.

If the promise of this thesis has been delivered upon, then we’ve seen that the law’s response to the Internet has been the creation of additional protections for interests that can be described as personhood interests. While these interests are not strictly new, in that they’ve all seen articulation in some form before, both their legal protections and the mechanisms by which they can be harmed have been expanded in the Internet context. Thus, I’ve termed their newfound protections to be “digital rights” to reflect the way the law has recognized, extended or created rights to protect these interests especially in the digital environment.

But for as much ground as has been covered, this thesis is only a small step in what I hope might become a more deeply-explored area of study. Much of this territory is new, and thus much must be done to lay the groundwork for future research. Indeed, even the division of theories of legal adaptation to technological change into the categories of procedural and substantive will hopefully focus research into those areas. Moreover, in Chapter 1, I attempted to create a taxonomy of the ways in which technological change can create cause for legal adaptation in a more complete way than has been devised in previous scholarship. This taxonomy can assist in understanding when, how, and why the law adapts to new technologies. I do not assert that this taxonomy is final, however, and the taxonomy may be refined through a more rigorous review of legal adaptations to technological change across a greater time scale and with consideration of

630 See Chapter 1, Part 3(b) supra.
631 I note Professor Bernstein’s work on genetic testing and the Internet as one exception: Bernstein, supra note 8.
more jurisdictions. Additionally, of course, I expect that not all will agree with the logic of my categorization.

Further, the methodology I have followed to assess legal adaptation to the Internet has only been roughly suggested in the literature, but not carried out in the manner of this thesis, in which a broad cross-section of legal adaptations were considered before being narrowed down to create a single substantive theory. While I believe that this method has proven useful, a practical problem arises here: addressing all of the legal adaptations to a technology as impactful as the Internet is singularly difficult. The review carried out in Chapter 2 was therefore cursory. However, in my view, even such a cursory review is useful in identifying trends, and for technologies that have spurred less legal adaptation, a rigorous review may be less daunting.

A few other quick comments regarding the theory are needed in order to address a few possible sticking points for the reader. In this thesis, I’ve developed a single substantive theory: that the law has been responsive to the personhood-expanding qualities of the Internet. More such theories are certainly possible, even from the same set of adaptations considered in Chapter 2. This thesis naturally focused upon a single distilled theme between the legal adaptations to the Internet, but that is not to say that there are not more, or that such themes might not be contradictory. Future research might apply this method again to the Internet to come to new conclusions and new insights. Needless to say, it might also be applied to countless more technologies.

The substantive theory itself, is, as the name suggests, quite theoretical. While my analysis of the interests protected by anonymity, limitations on copyright and defamation, and the interests being protected by anti-spam laws are grounded in substantial existing literature, the discussion of these as personhood interests, and my use of existential thought to define the notion of personhood, are perhaps less so. But I take existential thought—to the limited extent that I do—because it is, in my view, elucidating. The notion that we are in a state of constant meaning-creation and self-definition and that it is that fact that makes us persons, comports with an intuitive notion of self and with the notions of identity formation, human flourishing, and personal growth often mentioned in judicial decisions about privacy and freedom of

---

632 See Chapter 1, Part 3(b) supra.
expression. Of course, I take existential thought only so far, as I differ with many of its proponents’ prescriptive and descriptive claims. Nonetheless, an existential approach to personhood provides some illumination of why it is that certain rights and freedoms are important, and why it is that the Internet has become such a potent force for self-determination.

Furthermore, as I’ve noted previously, this thesis has taken a somewhat optimistic view of both the value of the Internet, which I do not expect to be controversial, and the legal adaptations to the Internet, which I expect to be somewhat more controversial. However, this is but one substantive theory of legal adaptation to the Internet, and the argument presented here does not preclude more pessimistic assessments of legal adaptation. The argument here might, on the other hand, serve to temper such pessimistic portrayals of cyberlaw by pointing out that there are trends towards protecting individual personhood, even if those trends might receive less attention than the realities of corporate and governmental abuses in the online arena. By identifying the ways the law has already protected personhood interests, it may also serve to provide a legal basis upon which future decision-makers can recognize, and potentially protect, the personhood interests at issue.

Some may also take issue with the notion that personhood is something that can be expanded by the creation of new technologies. It may be counterintuitive that modern people have more of that quality that makes them persons than those who lived in the distant, or even recent, past. However, I do not believe this should be surprising upon reflection. Can it not be said that those that live free from autocratic powers or forms of repression or slavery have more of what it means to be persons than those who live under their yoke? Then, can it not be said the same should apply to those who live longer by the virtues of modern medicine and sanitation, those who can know more and say more by virtues of modern communication, those who can explore the world and learn from more cultures and peoples by virtue of modern transportation, or those who can engage in more expression and creation by virtue of the many artistic mediums now available? Nothing in this revokes the status of persons from anyone, but simply asserts that those freedoms that define us as persons can be expanded or contracted through changes in the objective world.

---

633 See Generally Chapter 2, Part 3, supra.
And of course, the Internet has expanded those freedoms. By taking this view, we can not only understand the reasons for the rise of digital rights and the increased protections to digital interests on the Internet, but we can assess the importance and impact of new potential legal adaptations, such as virtual property rights, a right to one’s pseudonymous reputation, or a right to Internet access. We can also choose how best to regulate the Internet, such as whether we privilege anonymity over innovation in order to address Internet harms, or whether we favour net neutrality over market freedom. Each of these topics is a substantial one, worthy of further exploration and research from a personhood perspective.

Indeed, personhood interests are amongst the most fundamental of interests, and therefore some of the most worthy of protection. This assertion is hardly new or surprising. But if we’re serious about protecting these interests, it’s important that we understand how technologies impact them, how they expand our personhood, and how they make it vulnerable to new harms and new ways of inflicting old harms. By doing so, decision-makers can craft legal responses that reflect the proper balance of rights and interests while ensuring that people can obtain the full benefit of technological advancement.

---

634 I say “amongst” the most fundamental of interests, because there may be fundamental interests that are not personhood interests. Indeed, pure instances of happiness, pleasure, contentment, or other positive emotions are not themselves personhood interests under this framework, even if they are very important interests, and even if one chooses the pursuit of them as her purpose.
Bibliography

Legislation: Canada

Aeronautics Act, RSC 1985, c A-2.
Air Transportation Regulations, SOR/88-58
An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, SC 2010, c 23.
Canadian Aviation Regulations, SOR/96-433.
Copyright Modernization Act, SC 2012, c 20.
Criminal Code, RSC 1985, c C-46.
Electronic Transactions Act, SA 2001, c E-5.5.
Energy Efficiency Regulations, SOR/94-651.
Organizations in the Province of British Columbia Exemption Order, SOR/2004-220.
Organizations in the Province of Quebec Exemption Order, SOR/2003-374.
Personal Health Information Custodians in Newfoundland and Labrador Exemption Order, SI/2012-72.
Personal Information Protection and Electronic Documents Act, SC 2000, c 5.
Privacy Act, RSC 1985, c P-21.
Telecommunications Act, SC 1993, c 38.
Waste Electrical and Electronic Equipment, O Reg 393/04.

Legislation: United States

Computer Fraud and Abuse Act, 18 USC § 1030 (2012).
Electronic Fund Transfer Act, Pub L No 95-630, 92 Stat 3728.

Jurisprudence: Canada

Baglow v Smith, 2015 ONSC 1175, 110 OR (3d) 481, 350 DLR (4th) 694.
Barrick Gold Corp v Lopehandia (2004), 71 OR (3d) 416, 239 DLR (4th) 577 (Ont CA).
Irwin Toy v Quebec (Attorney General), [1989] 1 SCR 927.
King v Power, 2015 CanLII 11200 (NL SCTD).
R v Keegstra, [1990] 3 SCR 697.
R v NS, 2012 SCC 72, [2012] 3 SCR 726.
RJR-MacDonald Inc v Canada (AG), [1995] 3 SCR 199.
Warman v Wilkins-Fournier, 2010 ONSC 2126, 100 OR (3d) 648, 319 DLR (4th) 268 (Div Ct).

Jurisprudence: United States

America Online, Inc v IMS, 24 F Supp (2d) 548 (ED Va 1998).
Brookfield Communications, Inc v West Coast Entertainment Corp, 174F (3d) 1036 (9th Cir 1999).
Doe No 1 v Cahill, 884 A (2d) 451 (Del Supreme Ct 2005).
eBay Inc v Bidder’s Edge, Inc, 100 F Supp (2d) 1058 (ND Cal 2000).
Ferguson v Friendfinders, Inc, 115 Cal Rptr (2d) 258 (Cal App 1st Dist 2002).
Independent Newspapers, Inc v Brodie, 966 A (2d) 432 (MD 2009).
Intel Corp v Hamidi, 30 Cal 4th 1342, 71 P 3d 296 (Cal Sup Ct 2003).
Krinsky v Doe 6, 159 Cal App (4th) 1154 (Cal Ct App 2008).
MAI Systems Corp v Peak Computer, Inc, 991F (2d) 511 (9th Cir 1993).
Prater v Reichman, 135 Tenn 485 (Tenn Sup Ct 1916).
Sid & Marty Krofft Television Productions Inc v McDonald's Corp, 562 F (2d) 1157 (9th Cir 1977).
Thompson v Western States Medical Center, 535 US 357 (2002).
United States Telecom Association, et al v Federal Communications Commission and United States of America (14 June 2016), DC Cir, 15-106 (Ct App), online: US Court of Appeals for the DC Circuit
United States Telecom Association, et al v Federal Communications Commission and United States of America (14 June 2016), DC Cir, 15-106 (Ct App), online: US Court of Appeals for the DC Circuit
Wood v Hustler Magazine, Inc, 736 F (2d) 1084 (5th Cir 1984).

Jurisprudence: Other


Secondary Materials: Academic Articles and Essays

Bloustein, Edward J. “Privacy As An Aspect of Human Dignity: An Answer to Dean Prosser” (1964) 39 NYU L Rev 962.
Christiansen, Keith A. “Technological Change and Statutory Interpretation” (1968) 49:2 Wis L Rev 556.


Lawrence, Dan E. “It Really is Just a Game: The Impracticability of Common law Property Rights in Virtual Property” (2007-2008) 47 Washburn LJ 505.


——. “Understanding Legal Responses to Technological Change: The Example of In Vitro Fertilization” (2005) 6 Minn J L Sci & Tech 505.


Post, David G. “Against Against Cyberlaw” (2002) 17 BTLJ 1365.


Yim, Hannah Lee Fen. ““Virtual World, Virtual Land But Real Property” (2010) 2010 Sing JLS 304.


Secondary Materials: Books

Secondary Materials: Other


Hof, Rob. “Second Life’s First Millionaire”, Bloomberg Businessweek (26 November 2006), online:


Oliver, Donald in Debates of the Senate (Hansard), 37th Parl, 2nd Sess, No 140, Issue 77 (24 September 2003) at 1530 (Hon Donald H Olivier).

Oxford English Dictionary, OED Online.


