

TIME TO CARE ABOUT REPUTATION:
Re-Viewing the Resonances and Regulation of Reputation

jennifer barrigar

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

Graduate Studies in Law
Faculty of Law
University of Ottawa

©jennifer barrigar, Ottawa, Canada 2013

This work is licensed under the Creative Commons
Attribution-NonCommercial-NoDerivs 2.5 Canada License
<http://creativecommons.org/licenses/by-nc-nd/2.5/ca/>

ACKNOWLEDGEMENTS

This is dedicated to Carole Lucock, who never got to finish hers.

I am forever indebted and grateful to my supervisor, Dr. Ian Kerr for his unflagging enthusiasm, encouragement and insightful feedback. Working with Dr. Kerr has provided me with invaluable experiences, friendships and opportunities, among them the chance to return to university and pursue this doctorate.

Thank you also to Jane Bailey, Valerie Steeves, Shoshana Magnet, Constance Backhouse, Michael Geist, Elizabeth Judge and of course Ian Kerr for teaching, inspiration, assistance and challenge at various points during the process. Every experience I had within the University of Ottawa contributed in some way to the development of this project, and I am grateful to all of you who were part of that.

I must also acknowledge the opportunities, support and assistance received in support of this dissertation from the Social Sciences and Humanities Research Council (SSHRC); The University of Ottawa and the University of Ottawa Faculty of Law; the Canadian Council of Administrative Tribunals; the Office of the Privacy Commissioner of Canada; the Samuel-Glushko Canadian Internet Policy and Public Interest Clinic; Google; the Electronic Privacy Information Centre; and the Oxford Internet Institute.

Last but by no means least, my boundless gratitude to my families – both to my parents and siblings and to my chosen family here in Ottawa and elsewhere. Without your love, support, encouragement, periodic scolding and unflagging faith neither this project nor my surviving it would have been possible.

A final thanks to Zaphod Beeblebrox, the Dominion Tavern, Steamwhistle and Sourpuss for support of a different kind, though no less necessary or helpful.

ABSTRACT

This dissertation examines reputation as a regulating force in online and offline relationships and transactions, arguing that reputation requires protection through the promulgation of new laws.

Using John Locke's famous "under-labourer" approach as its central method, this dissertation ultimately sets out a series of conclusions, which form a preliminary framework upon which appropriate reputation regulation might be built.

Part I of this dissertation studies offers an interdisciplinary study of reputation. Chapter 1 examines the ways that reputation is created and maintained, the purposes for which it is used, and its role in risk management and trust. These understandings are then applied to reputation in process. Chapter 2 explores formal reputation systems and the ways in which user investments and desires become written into reputation such that multiple levels of "dominant" norms may be simultaneously operant. Chapter 3 shows this normative force also operating on social network sites, shaping identity performances. Finally, having established these intersections and the regulating power of norms upon reputation, the effect of such performances is examined in chapter 4, which identifies reputation's gatekeeper role in offline and online spaces and the risks this can create when information is accessed or employed without an understanding of the norms which have shaped that information. Thus reputation is shown as a socially negotiated and co-created process which exerts an unseen hegemonic force, with dominant political, economic and ideological interests embedded in seemingly social norms. These norms are enforced via reputation, which takes on a gatekeeper role, regulating access to a variety of spaces, information, and economic opportunities.

Part II begins with an examination of the current forms of legal and quasi-legal regulation of reputation that exist, ultimately finding that none of them is fully applicable to the complexity of reputation. Having established this complexity and shown that current approaches are inadequate, chapter 6 moves on to examine and then reject the neoliberal approach currently applied to these issues, finding its focus on individual responsibility to be inadequate and inappropriate, calling instead for a mode of regulation that understands reputation within its social context.

Table of Contents

Introduction	1
Introducing Reputation.....	4
Increasing Reliance on Reputation	6
Why Inquire Further?	8
The Under-labourer	11
Clearing the Technological and Legal Underbrush: Methodology	12
The Path Forward	16
CHAPTER 1:	19
Situating the Discussion: Norms, Trust and Reputation	19
Norms	21
Norms and the Derivation of Reputation	25
Preliminary Exploration of Trust.....	26
Extensions of Reputation and Trust	27
Reputation as Proxy for Trust	29
The Role of Trust.....	31
The Goal of Trust	32
Extending Trust to Online Spaces	33
Surveillance.....	34
Conclusion	38
CHAPTER 2:	40
Creation, Embedding and (re)Enforcement of Community Norms via Reputation Systems	40
Participatory Surveillance	41
Reputation Systems as External Surveillant Force	46
Panopticism	46
Is Reputation Panoptic?.....	48
Parsing Participatory Reputation Systems	51
Synopticism.....	55

Synoptic Forces in Reputation	58
EXAMPLE 1: COMMUNITY DERIVED NORMS: Ebay	61
EXAMPLE 2: MAINSTREAM NORMS: INTERNET DATING	64
EXAMPLE 3: USER DETERMINED CONTENT: DIGG	67
Creation of the Transoptic Norm.....	70
Conclusion	72
CHAPTER 3:	74
Non-Systematized Impression and Reputation Management	74
Social Network Sites	74
Profiles and Identity.....	76
Performative Identity	79
The Technosocial is the Social	82
Impression Management.....	84
Authenticity	89
Conclusion	92
CHAPTER 4: Out of Context:	96
External Uses of Reputation Information	96
Mediated Publics	97
Audience and Context	99
External Uses of Online Information	108
EMPLOYMENT.....	108
EDUCATION.....	112
THE COURTS.....	114
LAW ENFORCEMENT.....	119
STATE	121
Information Analysis.....	123
Denial of Access	123
Managing Reputation	128
CHAPTER 5:	131
Existing Legal Frameworks for Reputational Governance	131
Scope of Harm	132
Current Legal Approach: <i>Criminal Code</i>	135

Current Legal Approach: Privacy Legislation	141
Current Legal Approach: Private Law	144
Conclusion	163
CHAPTER 6: Stupid User:	165
Re-Viewing and Re-Placing Responsibility	165
Introducing the Stupid User	165
Presumptive Publicness and the Stupid User	167
A: STAPLES	167
B: NATHALIE BLANCHARD.....	170
C: CORPORAL BROWN	170
WHY ARE THESE USERS “STUPID”?.....	172
Law & Society.....	173
Governmentality	174
Responsibilization	176
Reputation and Responsibilization	185
GOVERNMENT	186
ADMINISTRATIVE	195
COMMERCIAL	199
INDIVIDUAL.....	203
The Stupid User as the Responsibilized Individual	204
Conclusion	211
CONCLUSION:	214
Towards a Framework for Reputational Governance	214
Mandate	214
Deconstructing Norms.....	216
Distinguishing the Existing Approaches.....	216
Valuing Reputation	217
Towards a Framework for Reputational Governance	219
Established Points:.....	219
The Need for Law:.....	220
CONCLUSION 1.....	221
Aspirational Approach	221

CONCLUSION 2.....	223
Scope of Law	223
CONCLUSION 3.....	224
Focus.....	224
CONCLUSION 4.....	225
Identifiability.....	225
CONCLUSION 5.....	227
Is Takedown Sufficient?	227
CONCLUSION 6.....	228
Equity-based Approach.....	228
CONCLUSION 7.....	230
CONCLUSION 8.....	230
CONCLUSION 9.....	230
Elements of the Framework	230
Bibliography	233
Laws	233
Jurisprudence	234
Reports.....	235
Speeches.....	236
Guidance Documents	237
Secondary Sources: Books	237
Secondary Sources: Articles.....	241
Online: Blogs, Articles & Resources	252

TIME TO CARE ABOUT REPUTATION:

Re-Viewing the Resonances and Regulation of Reputation

*An' I don't give a damn 'bout my bad reputation
Never said I wanted to improve my station
An' I'm only doin' good
When I'm havin' fun
An' I don't have to please no one¹*

Introduction

In 1979, Joan Jett was adamant that she didn't give a damn about her bad reputation. Indeed, the bad reputation that she celebrated was a source of pride as well as (or perhaps because it was) one garnered by behaving outside the normative female role. The singer acknowledges that she has been tagged with a 'bad reputation' because of the way she behaves, but instead of being shamed by it she argues that the standards against which she's being judged are archaic, that her freedom and search for fun is emblematic of her (new) generation and that people can say whatever they want and it won't make a difference anyway, not just to her but in the larger world. It's a strong message and one that has achieved huge cultural resonance, appearing in movies, tv shows, video games, as well as being covered by a variety of other artists. In 2009, VH1 put 'Bad Reputation' at #29 on the list of the top 100 rock songs.²

Anthemic though the song (and message) may be, while Joan Jett may not have cared about her bad reputation, these days that option is both less possible and less desirable. That is because reputation is increasingly a valuable and valued commodity, a key indicator of trustworthiness and a potential granter of access. No longer will it 'not make a difference' when 'people say what they want to say', indeed, it is exactly what people say and do that creates and enforces reputation, good or bad.

¹ Joan Jett, Richie Cordell, Kenny Laguna, Marty Joe Kupersmith. "Bad Reputation". *Bad Reputation*. Boardwalk Records 1981.

² <<http://music.spreadit.org/vh1-top-100-hard-rock-songs/>>.

Concerns about Online Information

As of 30 June 2012, there were 2,405,518,376 internet users across the world, over 34% of the total world population.³ Within those billions of users, almost 95% of American teens are using the internet and 78% of adults are doing so.⁴

The extent to which internet use has permeated the world is noteworthy. So too is the speed of the permeation. The 2,405,518,376 number represents a growth of 566% since the year 2000.⁵ This kind of exponential growth as well as cross-age permeation inevitably brings with it new issues and a necessity of re-viewing old issues.

The issue with which this project is engaged is the use and resonance of reputation and ranking systems.

There are many studies and surveys that seek to collect the perceptions and experiences of internet users for re-view and analysis. Recent studies show that 4% of adults⁶ and 18% of teens indicate that they have “been embarrassed or disciplined as a result of showing something on a social network.”⁷ This is not to say that anything posted to the internet or on a social network site is automatically problematic. Rather, it is when information (in the form of writing, photos, videos, or any other personal information) is not only public, but is viewed by others and some kind of normative

³ INTERNET USAGE STATISTICS, The Internet Big Picture: World Internet Users and Population Stats, online: <<http://www.internetworldstats.com/stats.htm>>

⁴ Amanda Lenhart, Mary Madden, Aaron Smith, Kristen Purcell, Kathryn Zickuhr, Lee Rainie, “Teens and Digital Citizenship Survey: Teens, Kindness and Cruelty on Internet Sites” Pew Internet and American Life Project (Nov 9, 2011), online: <<http://pewinternet.org/Reports/2011/Teens-and-social-media.aspx>> at 15.

⁵ *Ibid.*

⁶ *Ibid.*

⁷ TRUST-E, “The Kids Are Alright: a survey of the privacy habits of teens and their parents on social networks” (October 2010), online: <http://www.truste.com/pdf/TRUSTe_SNS_shortdeck.pdf> at p 10>.

assessment is attached to that information that damage may occur in the form of harm to the individual's reputation.⁸

Whether as a result of having experienced such repercussions, or simple awareness of them, other research indicates that teens are aware of the possibility that their social media interactions and contributions may have an impact on them. A recent Pew survey showed that almost half of all teen internet users had at some point withheld or at least reconsidered posting something online, with older teens being more likely than younger to do so.⁹

This becomes of particular interest when the various uses to which information on the internet may be put are examined. It appears that up to 44% of adults online have used internet information to find out more about someone they were considering hiring in a professional capacity. Interacting in a non-professional capacity appears to be no guarantee of exclusion from such searches; 31% of internet users with jobs have gone online to find information related in other ways to employment, be it about co-workers, colleagues or competitors. Completely outside the world of employment, the internet appears still to be a popular tool, with 34% of online dating site users using internet searches to find information about potential partners. Of those who are not using internet dating sites, the internet is still used to find information about an individual as part of dating or a relationship by 16% of users. Other personal uses of

⁸ Common Sense Media, "Social Networking Tips" (Oct 17, 2011), online:

<<http://www.commonsensemedia.org/advice-for-parents/social-networking-tips>>.

⁹ "Older teen internet users (ages 14-17) are more likely than younger teens (ages 12-13) to say they have reconsidered posting content online after thinking about the possibility of negative implications (59% vs. 46%)." This continuum of awareness and care over information sharing appears to fall along age lines, with 67% of 17 year olds – the oldest group studied – indicating that they had decided to withhold something due to concerns about the impact it might have on their reputation: Amanda Lenhart, Mary Madden, Aaron Smith, Kristen Purcell, Kathryn Zickuhr, Lee Rainie, "Teens and Digital Citizenship Survey: Teens, Kindness and Cruelty on Internet Sites" Pew Internet and American Life Project (Nov 9, 2011), online: <<http://pewinternet.org/Reports/2011/Teens-and-social-media.aspx>>.

such searches include seeking out information about friends, neighbours and various people from their pasts (by up to 46%).¹⁰

Protection and Online Information

Surely individual awareness of risks and the attendant decision(s) to assess information and withhold things that might be problematic should be sufficient protection against negative repercussions? Alas, it is not that simple, because information you post online about yourself is not the only information that may be accessed in an internet search. Thus, no matter how careful anyone may be about what content they make public, they can't exercise the same care over what friends, acquaintances and others may put online. Given this, it seems that increasingly – no matter how careful they are about their own disclosures, even to the extent of not putting up anything – people feel a necessity to monitor all information available about themselves online, no matter where or by who posted. Accordingly, it is not a surprise that self-monitoring is increasingly a part of maintaining an online presence, with 57% of online adults reporting the use of search engines to review what information about themselves is available online.¹¹

Introducing Reputation

As discussed above, research has shown that adults, young adults and children are or may be subject to repercussions stemming from personal information available about them online. When people report experiencing negative repercussions from information posted online, they can mean many things, both immediate and long-term.

¹⁰ Mary Madden, Aaron Smith, "Reputation Management and Social Media" Pew Internet and American Life Project (May 26, 2010), online: <<http://www.pewinternet.org/Reports/2010/Reputation-Management/Summary-of-Findings.aspx>>.

¹¹ Mary Madden, Aaron Smith, "Reputation Management and Social Media" Pew Internet and American Life Project. (May 26, 2010), online: <<http://www.pewinternet.org/Reports/2010/Reputation-Management/Summary-of-Findings.aspx>>.

Information posted online can be anything – status reports, pictures, videos, comments on a Facebook wall, group memberships, sites or products that have been “liked”, even something as simple as an inside joke that gets misinterpreted by someone looking at it from outside. And no matter how unobjectionable it may seem to the poster, just as you have no control over what someone else may post¹² you also have no control over how someone else may interpret information and what inferences they may draw from it.

The problem is in how people respond to things they perceive negatively. Negative repercussions stemming from information or based on inferences drawn from that information and its availability may be fairly direct, for instance, a parent finding out about a planned party or a teacher finding out the actual activities of a “sick” student. Increasingly, however, the negative repercussions have long-term and more dispersed resonance. They become not just an isolated reaction to one piece of information, but rather get incorporated into an assessment of the individual overall. Thus, when people react negatively to some piece of information they see or hear, that negative perception is incorporated into the image that person has of you. It is also likely to be conveyed to others – perhaps not the information or incident itself but certainly the negative impression – which as it is shared, becomes part of the perception about you, not just on the part of one person but on the part of those s/he interacts with and shares information and impressions with.

When others use information about an individual as a basis for decision making, they are extrapolating from that information in order to form an opinion or judgement of the individual, or (in the case where the individuals are already known to each other) to inform or bolster an opinion or judgement of the individual. This is not an unknown

¹² There are, of course, privacy controls that will allow someone to exercise some control over information about them, whether it is what can be posted on their wall/timeline or the necessity of approving posts for the timeline before they are published, but no control provides an absolute guarantee that someone else won’t post something on their own timelines that identifies or appears to identify you.

phenomenon, but rather one with which we are intimately familiar under the name “reputation”.

The link between repercussions experienced as a result of information made public and reputation (bad or good) is, then, that at its most basic, reputation is comprised of a record of interactions and past experiences. As Donath and boyd observe, “[m]ost of the qualities we are interested in about other people – is this person nice?

Trustworthy? Can she do this job? Can he be relied on in an emergency? Would she be a good parent? – are not directly observable. Instead, we rely on signals, which are more or less reliably correlated with an underlying quality.”¹³ Thus, when online information is collected, consulted or in some other way integrated, into a decision-making process about an individual, it is reputation, in some form, that is at issue. Conte & Paolucci note that “reputation” is a concept that appears across cultures and time periods; from Ancient Greek and Roman histories, through aboriginal groups including Canadian First Nations, American Indians and Bedouin tribes, and in related form, in Asian cultures.¹⁴ Aphorisms regarding reputation are present in our literature¹⁵ and the proverbs that form part of our cultural and moral history.

Increasing Reliance on Reputation

As our society becomes increasingly dispersed – both geographically and spatially (moving to online spaces) – people are increasingly dealing with those they do not know or do not know well. In order to facilitate those dealings and encourage comfort with ecommerce and other social, economic and political interactions, that uncertainty between strangers must be addressed.

¹³ Judith Donath & danah boyd, "Public Displays of Connection", Book Review of 71 by (2004) 22:4 BT Technology Journal at 71.

¹⁴ Rosaria Conte and Mario Paolucci, "Reputation in Artificial Societies: Social Beliefs for Social Order." *Multiagent Systems, Artificial Societies, and Simulated Organizations*, edited by Gerhard Weiss (2002) at 16.

¹⁵ W. Shakespeare, *Hamlet*; *Othello*.

Increasingly, reputation has become a tool used to bridge that gap. Reputation is, after all, a record of interactions with an individual and impressions gleaned from those interactions. Thus, when contemplating dealing with an unknown person or entity, their reputation may be consulted in order to (help) determine whether or not to enter into the transaction.

Although “transaction” carries with it the flavour of business (and reputation is certainly being used in commercial circumstances), there are many exchanges that take place outside of commerce an reputation is or can be instrumental in all of them. Just as some online commerce sites are attaching feedback ratings to users, so too are formal and informal feedback consulted when it comes to permitting access to spaces, to services, and to information in certain circumstances.

It is for this reason that reputation is an issue that must be examined. Although reputation has always fulfilled this gatekeeper function locally, it is now expanding; more people are interacting with each other, meaning there is more, and dispersed, input into the derivation of reputation and that reputation is in turn being consulted more often and used to make decisions in an increasing number of areas.

We have a situation, then, where (1) your reputation is developed based on what other people say and think about you; (2) that reputation is increasingly available anywhere and to anyone; (3) your reputation is used to make decisions about you, whether to hire you, whether to enter into business with you, whether to let you enter into a protected or private conversation; and (4) you may not know what that reputation is, you may not know who is consulting it, and you aren’t able to do anything to change or challenge the reputation if you feel it to be false or unwarranted.

So yeah, Joan Jett may not have cared about her bad reputation, but increasingly, a bad reputation matters. It matters because it governs access to spaces, to information, and to social, political and economic participation. And because the trends suggest that reputation is only going to become more ubiquitous, not less.

Currently, research indicates that to date, self-monitoring has been reasonably effective. Indeed, only 8% of adult internet users report having to request the removal of information about them, and 82% of those indicate that those requests have generally been successful.¹⁶

While these statistics – both the low incidence of problematic information and the relative ease of redressing the problem – are encouraging, they should not be taken to indicate that there is not now, nor will there ever be, problems in this arena that require legal examination and redress. Indeed, the more common reputation becomes as a tool, the more inevitable it seems that the area will become one where self-monitoring is not and should not be the appropriate form of regulation.

Why Inquire Further?

Alright then, we know reputation is a problem; let's just draft a law to deal with the issue and move on. Why not? Well, to put it bluntly, because it's important to write the right law, not just a law.

The *Video Privacy Protection Act*¹⁷ was drafted and passed by the US Congress after a media outlet acquired and published Robert Bork's videotape rental history during his nomination to the US Supreme Court. It protects the privacy of information about rentals of "pre-recorded video cassette tapes or similar audio visual material."¹⁸ As it is, the Act stands as a great example of the failure of law to deal effectively with technology. That is, in the wake of a perceived violation of privacy, legislation was

¹⁶ Amanda Lenhart, Mary Madden, Aaron Smith, Kristen Purcell, Kathryn Zickuhr, Lee Rainie, "Teens and Digital Citizenship Survey: Teens, Kindness and Cruelty on Internet Sites" Pew Internet and American Life Project (Nov 9, 2011), online: <<http://pewinternet.org/Reports/2011/Teens-and-social-media.aspx>>.

¹⁷ (1988) 18 USC §2710, <<http://www.law.cornell.edu/uscode/text/18/2710>> (VPPA).

¹⁸ Although the Act has been cited in a recent class action suit, arguing that it applied to DVD and similar media, the case resulted in a settlement, with the result that there is still no court recognition of the Act applying to any media besides VHS tapes. Case No. 5:11-CV-00379 EJD; United States District Court, Northern District of California, San Jose Division.

drafted and passed to deal with that particular technology and prevent that particular kind of violation from recurring. Thus, although the Electronic Privacy Information Centre describes the Act as “one of the strongest protections of consumer privacy against a specific form of data collection”¹⁹, it also stands as a lost opportunity to apply strong privacy protections against data collection more broadly.

The ongoing saga of “lawful access”²⁰ in Canada seeks to capitalize on concerns about overly technology-specific legislation by casting its net extremely broadly. First introduced by the Liberal government in 2004, lawful access has now been introduced and failed on the Order paper twice by the Conservative government as well.

Need for this legislation, according to the Department of Justice, is because:

While technology has evolved considerably since then, Canada's lawful access laws have not kept pace. Increasingly complex technologies are challenging conventional lawful access methods. Criminals and terrorists are taking advantage of these technologies to assist them in carrying out illicit activities that threaten the safety and security of Canadians. To overcome these challenges, legislative tools, such as the *Criminal Code* and other statutes, must evolve so that law enforcement and national security agencies can effectively investigate criminal activities and threats to national security while ensuring that Canadians' privacy and human rights are protected.²¹

The Privacy Commissioner of Canada has responded to these claims by arguing:

Despite repeated calls, no systematic case has yet been made to justify the extent of the new investigative capabilities that would have been created by the bills. Canadian authorities have yet to provide the public with evidence to suggest that

¹⁹ <<http://epic.org/privacy/vppa/>>

²⁰ Ian R. Kerr, Daphne Gilbert, and Jena McGill, "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers" 51:4 *Criminal Law Quarterly* 469-507(2006). Available at SSRN: <http://ssrn.com/abstract=1302544>

²¹ Department of Justice (2005) Lawful Access FAQ: <<http://www.justice.gc.ca/eng/cons/la-al/sum-res/faq.html>>

CSIS or Canadian police cannot perform their duties under the current regime. One-off cases and isolated incidents should not prove the rule, nor should exigent or emergency circumstances, for which there are already *Criminal Code* provisions.

As well, if the concern of law enforcement agencies is that it is difficult to obtain warrants or judicial authorization in a timely way, these administrative challenges should be addressed by administrative solutions rather than by weakening long-standing legal principles that uphold Canadians' fundamental freedoms.

I am also concerned about the adoption of lower thresholds for obtaining personal information from commercial enterprises. The new powers envisaged are not limited to specific, serious offences or urgent or exceptional situations. In the case of access to subscriber data, there is not even a requirement for the commission of a crime to justify access to personal information – real names, home address, unlisted numbers, email addresses, IP addresses and much more – without a warrant. Only prior court authorization provides the rigorous privacy protection Canadians expect.

In my view, the government has not convincingly demonstrated that there are no less privacy-invasive alternatives available to achieve its stated purpose.²²

Though coming at the problem from (nominally) opposite directions, the examples provided by the VPPA and by Canada's failed lawful access initiatives emphasize the need to approach questions of technology and regulation in a balanced way, neither too broadly nor too narrowly to provide effective and appropriately focussed regulation.

As Easterbrook notes, the best path forward is not to "struggle to match an imperfect legal system to a technology we understand poorly. Let us instead do what is essential in this evolving world to allow participants to make their own decisions."²³ It is in order to create the conditions necessary to identify what is essential that this project is undertaken.

²² Jennifer Stoddart "Letter to Minister of Public Safety Vic Toews" (2011) <http://www.priv.gc.ca/media/nr-c/2011/let_111027_e.asp>, reiterated in a letter to the editor 7 November 2012 <http://www.priv.gc.ca/media/nr-c/2012/an_121107_e.asp>

²³ Frank L. Easterbrook "Cyberspace and the Law of the Horse" (1996) U. Chicago Legal F 207 at 210

The Under-labourer

Having recognized that online information about an individual (whether posted by themselves or others) may have negative effects upon that individual, some mechanism for controlling that information and those effects is necessary.

That said, the VPPA certainly, and arguably lawful access as well, demonstrate that attempting to regulate issues related to technology is a project that contains within it inherent dangers; misunderstanding the technology or its scope and focussing too narrowly or too broadly in scope, for a start. It is important, therefore, that any project which has such regulation as its goal proceed carefully.

Luckily, there is a template of sorts for such a project, and it can be found in John Locke's *An Essay On Human Understanding*, particularly in his discussion of the role of the "under-labourer" as set out in the *Epistle to the Reader*.²⁴ In the essay as a whole, Locke seeks to examine and articulate the process(es) of thought and perception, arguing that knowledge is a product of experience rather than a pre-existing thing. That is, that objects are actually a bundle of perceptions around which we create language and to which we impute an underlying objective being or truth.

The Epistle serves as an introduction, wherein Locke relates the genesis of this inquiry (a philosophical discussion with a half dozen friends) and the processes and revelations that followed upon that evening, especially with regard to the importance of experience and perception and their individual nature(s) in shaping thought and knowledge. He is at great pains to emphasize the modesty (false or otherwise) of his project in publishing these thoughts. He notes that his intended audience are not those who already know great truths, but rather those "men of my own size, to whom, perhaps, it will not be unacceptable that I have taken some pains to make plain and familiar to their thoughts some truths which established prejudice, or the abstractedness of the

²⁴ John Locke "An Epistle to the Reader" *An Essay Concerning Human Understanding*, ed. P. Nidditch (Oxford, Clarendon Press, 1975) at 9. See also: <<http://www.ilt.columbia.edu/publications/Projects/digitexts/locke/understanding/epistle.html>>.

ideas themselves, might render difficult.”²⁵ Instead of purporting to be one of the “master-builders” he so admires, Locke proposes instead to take on the mantle of the under-labourer, recognizing that:

...the commonwealth of learning is not at this time without master-builders, whose mighty designs in advancing the sciences, will leave lasting monuments to the admiration of posterity; but everyone must not hope to be a Boyle, or a Sydenham; and in an age that produces such masters as the great Huygenius, and the incomparable Mr. Newton, with some others of that strain; it is ambition enough to be employed as an under-labourer in clearing the ground a little, and removing some of the rubbish that lies in the way to knowledge.²⁶

The aim of the under-labourer, then, is not to strive to create something new, groundbreaking and world-changing. Instead, grounded in his recognition of the way that experience and perception may act to shape knowledge, Locke proposes to clear the way to knowledge; to work as a kind of intellectual groundskeeper, clearing away the underbrush and weeds that choke new growth in order to create a clear path and facilitate healthy growth.

Clearing the Technological and Legal Underbrush: Methodology

The number of persons in online spaces, the degree to which use of those spaces has proliferated, and the incredible rate at which these technologies and spaces have permeated everyday life has, as previously stated, created a situation where new issues will arise and established issues and solutions may need to be re-viewed in order to ensure that they are being dealt with appropriately in all the circumstances. That is, as reputation becomes more ubiquitous, existing issues with reputation will likely continue to be relevant, but the expansion will inevitably result in new issues and

²⁵ John Locke “An Epistle to the Reader” *An Essay Concerning Human Understanding*, ed. P. Nidditch (Oxford, Clarendon Press, 1975) at 9. See also:

<<http://www.ilt.columbia.edu/publications/Projects/digitexts/locke/understanding/epistle.html>>.

²⁶ John Locke “An Epistle to the Reader” *An Essay Concerning Human Understanding*, ed. P. Nidditch (Oxford, Clarendon Press, 1975) at 9. See also:

<<http://www.ilt.columbia.edu/publications/Projects/digitexts/locke/understanding/epistle.html>>.

concerns. As such, care is needed in assessing the issue. It will not be sufficient to presume that existing methods of regulation are sufficient now or that they will continue to be sufficient.

The sources of information that will build the path must also be carefully selected to be appropriate to the task. In the introduction to his “Metaphors of Multiplicity”, Roderick A. MacDonald notes that most disciplines within the academy are aware of and comfortable with a variety of approaches shared between disciplines, while “legal scholars, by contrast, are so committed to the systematic singularity and coherence of law”²⁷ that they have a tendency to dismiss the contributions and knowledge of other disciplines. It is a recognition that is particularly apt at the beginning of this under-labourer’s task. That is, if Locke is correct that preconceptions have the power to shape perception and thus that the under-labourer’s task is to strip away the detritus (including preconceptions) in an attempt to clear a path to uncluttered knowledge, then it would be counter-intuitive to seek a path or an answer to this issue within a single discipline, especially one known for singularity of vision and focus.

The broad context of this project is an interdisciplinary investigation of reputation – its derivation, uses, resonances and regulation. This underscores the goal of making visible the complex social, technical and political nuances embedded within reputation.

In Code 2.0, Lawrence Lessig argues that not only is the regulation of technological spaces necessary and inevitable, but that there are already regulatory protocols operating within those spaces. Eschewing a narrow understanding of regulatory force that focuses exclusively on law, Lessig instead brings forward a fourfold understanding of regulatory force, one that posits law, market, norms and architecture as all shaping and placing constraints upon behaviour.²⁸ The original research question upon which

²⁷ Roderick A. MacDonald, “Metaphors of Multiplicity: Civil Society, Regimes and Legal Pluralism” (1998) 15 *Ariz J. Int’l and Comp L* 69 at 69.

²⁸ Lawrence Lessig. *Code Version 2.0* (2006, Perseus: New York) at Ch.7

this thesis is founded is rooted firmly in this perspective – that is, the concern about the normative force exerted by reputation systems is grounded in the recognition of the regulatory force of norms as well as the way(s) in which norms may be built into site architecture in a way that operationalizes them while simultaneously rendering them invisible.

In order to investigate this concern, this work is informed by two methodological priorities: first, the development of a contextual understanding of the evolution and use of discourses about “reputation”; second, an attempt to destabilize hegemonic discourses surrounding reputation and identity performance.

The quest to appropriately reflect the development and use of discourses about reputation as well as their limitations is one that is undertaken in a progression. Initially, a strategic decision is made; to begin by presenting the most charitable case of the proposition(s) that can be examined and nuanced – reflecting back the unproblematized and instrumentalist views of reputation and reputation technologies as represented in mainstream discourse.

These views were ascertained via a survey of contemporary media and scholarly articles which focussed directly on reputation and formal reputation systems. The review facilitated the development of a preliminary taxonomy of relevant terms (identity; reputation; risk; trust; security). This developed taxonomy was then used as a framework for a literature review; first to identify relevant academic disciplines (social science; philosophy; psychology; and communications) and then to identify literatures and authors of interest. With this as a prelude, an instrumental approach was then employed in performing a trans-disciplinary literature review, one that built upon the taxonomy to develop a conceptual framework of the fundamental issues involved in reputation.

Building upon this, a re-view of identity negotiation and presentation is used to gradually complicate this (simplistic) position, revealing the intricacies of techno-social

interactions in order to show the full complexity of the subject matter. This project is continued in Part 1 as the subject matter understanding is transformed from that unproblematic and instrumentalist position to a holistic understanding of reputation that incorporates recognition of both its normative force and gatekeeper function.

Using the narrow confines of a formal reputation system, I begin by examining the ways in which reputation is constructed and implemented. The clearly delineated boundaries of the formal system facilitate a deconstruction of the reputation creation process that allows the various norms and perspectives embedded in a single reputation ranking to be identified and elaborated upon.

Having parsed the construction of reputation, the idea is then examined within the socially dynamic context of a social network site in order to show how reputation works, and how the norms embedded within reputation come to exert a regulating force in shaping identity negotiation and performance. This part of the analysis results in a new understanding of reputation as a dynamic and technosocial process that exerts a normative force.

Having established how reputation is constructed and how it operates as part of dynamic social interactions, the final step of this stage of the project examines the way(s) in which reputation is and can be used to restrict access to opportunities, information, and economic and civic participation, and thus why the disruption of this hegemonic force must necessarily engage the scrutiny of law and policy makers.

At this stage, reputation has been fully parsed and grounded, its construction and use identified and its potential impacts surveyed. This is not, however, the end of the inquiry. Locke's under-labourer didn't seek to clear away debris and confusion merely for the sake of understanding. Rather, the project of clearing was in order to provide a clear path to knowledge. In this case, having cleared the path of misunderstandings by seeking to fully understand the issue, the inquiry must then progress along the path to knowledge.

The focus of the analysis then shifts away from the creation and operation of reputation and towards the regulatory role(s) of law and policy. This shift of focus brings with it a shift in methodological approach, moving to use a Foucaultian understanding of the structures of power as the lens through which various approaches to governing reputation are viewed and re-viewed. This stage of the analysis, then, begins with a review of the way(s) that reputation or aspects of reputation are currently being regulated (if at all), either legally or extra-legally. It then proceeded to identify and examine current governance strategies and the identification and critique of various approaches in order to assess their efficacy in appropriately addressing the issue. This in turn leads to the identification of features that should be addressed in any regulatory scheme for reputation.

The Path Forward

The first part of the project, then, will necessitate developing a full understanding of reputation. Accordingly, chapter 1 sets out the basics; seeking to understand what reputation is, how it is derived and with reference to what and, ultimately, what function it fulfills.

Having grounded an understanding of reputation, chapters 2 and 3 will then look at how identity is negotiated and re-negotiated within social interaction(s). Looking at formal reputation systems in chapter 2, and then at informal social interactions that lead to reputation in chapter 3, an understanding of the forces that shape both our self-presentation and the formation of reputation is pursued.

The final chapter of Part I, chapter 4, examines the question of how this complex reputation, that is now understood, functions and whether harm could result from that functioning, and what that harm might encompass.

After establishing in Part I a deep understanding of the complexity of reputation and of the risks implicit in unregulated reputation, Part II moves to examine the existing approaches to reputation regulation.

First, chapter 5 reviews the existing legal mechanisms that might apply to some or all aspects of reputation in order to assess whether they are addressing the issue adequately.

Not content to rely solely on law as a regulating force, chapter 6 then attempts to examine other forms of regulatory power that may shape reputation and its regulation.

At the end of this process, it is my hope that the under-labourer's task will be complete. That a holistic and informed understanding of reputation will have been developed, one that places the issue within the social, political and economic contexts that shape reputation, and that from that understanding it will be possible to identify the elements that must be present in any regulatory framework that is to address the issues around reputation appropriately and effectively.

CHAPTER 1:

Situating the Discussion: Norms, Trust and Reputation

The first part of the project of the under-labourer, then, is to seek to understand her subject fully and completely – only by so doing can the ground clearing process be effective, correctly identifying what is rubbish and what is not.

As discussed in the introduction, studies that show adults and teens suffering negative repercussions from information publicly available online demonstrate that reputation is an emerging and important issue, however, the link between repercussions and reputation has not yet been grounded. Accordingly, in this first chapter I will pursue the aims of (1) looking at the interrelationship of social interaction, information sharing, trust and risk-analysis and reputation; and (2) in the course of that, make explicit the link between information, reputation, and repercussions.

The idea of reputation is one that can be seen in multiple cultures, time periods, and forms. In order to understand reputation, however, it is important to interrogate exactly what is meant by “reputation”, how it functions, and what its composite processes are.

Nock defines reputation as:

...a shared, or collective, perception about a person. It is the product of the innumerable contacts among and between people. Through our dealings with others, an image is developed of the degree to which I do or do not conform to the standards that matter to them. Those who enjoy a “good” reputation are thought

to accept and abide by those standards – perhaps even demonstrating extraordinary conformance to them²⁹

Thus, reputation is not immutable – rather, it is dynamic, is composed of a number of different aspects and is used for multiple purposes.

In the following chapter, I will explore the interrelationships between social norms, risk assessments, trust and risk assumption in order to show both how reputation functions and its intersection with trust and risk-aware culture. I will demonstrate that trust is the result of individual risk-assessments conducted on the basis of sufficient, reliable and available information. In order to explore the meaning and role of reputation in this assessment, it is necessary to establish the following:

First, I will examine the role of social norms in constructing behaviour. In order to do so, I will examine the meaning of social norms, the behavioural implications of internalization of norms, and the ways in which norms both are enforced and act to enforce desired or expected behaviour.

Having shown these separate processes, I will proceed to examine the role of norms in the derivation of reputation, arguing that reputation may consist of or be constructed upon inter-community assessments of norm-conformance.

Next, the notion of trust will be interrogated in order to understand what trust encompasses and what processes it entails.

Reputation, however, has a dual nature. Having considered reputation as the result of shared signals or assessments, I shall then examine the role reputation plays in trust

²⁹ Steven L. Nock, *The Costs of Privacy: Surveillance and Reputation in America* (New York: Aldine de Gruyter, 1993) at 2

formation, functioning as a signal in its own right. In this way, the idea of reputation as a proxy for trust will be proposed and explored.

The relationship between trust and reputation will then be considered by looking at the role of risk-assessment in producing trust. This culminates in the recognition of trust not as an object bestowed, but as a limited product of risk-assessment.

Finally, having explored this trust and reputation interrelationships offline, the chapter will introduce the role of trust in online spaces by discussing the surveillant force of reputation.

Norms

When I speak of norms – in this case, of social norms – I refer to the behavioural expectations for effective participation in society. That is, a set of behavioural expectations that, when met, enable positive or desired interaction with others. Obviously norms are variable – not only does each society develop and enforce its own norms, but even within a given society or community there may be a multiplicity of seemingly contradictory norms and expectations to be navigated.³⁰

Norms are expectations, and are, therefore, distinct from laws. While laws (or rule norms³¹, as Conte & Paolucci would have it) are created and enforced by a central authority, norms are social constructions, the product of unspoken negotiation and collective awareness. This is not to say that norms are not enforced. Indeed, norms are enforced both implicitly and explicitly, not necessarily via a central authority but within the community, through ongoing social interaction as they open up and close down possibilities for transactions or other forms of interaction with others.

³⁰ Lawrence M. Friedman, *Guarding Life's Dark Secrets: Legal and Social Controls Over Reputation, Propriety and Privacy* (Stanford: Stanford University Press, 2007) at 2 - 4

³¹ Rosaria Conte and Mario Paolucci "Reputation in Artificial Societies: Social Beliefs for Social Order." In *Multiagent Systems, Artificial Societies, and Simulated Organizations*, edited by Gerhard Weiss,(2002) at 85.

Social norms are promulgated and enforced through social interactions, with majority community expectations exerting the power of the community, often via gossip. While gossip may be conventionally defined as idle talk or rumour³², instead it can be argued that gossip functions as an information exchange that promulgates, re-states, maintains and enforces social norms.³³ This happens in different ways.

First off, norms are maintained and enforced through shaming. This may be confrontational, as with individuals who actively confront norm-breakers³⁴, or it may happen through the force of gossip, with no actual confrontation needed. In either case, shame acts to stigmatize those who transgress norms, while the threat of shame deters other individuals from such transgressions. It is important to note, too, that the shaming is targeted at the individual, not the action.³⁵

Norms do not solely work through external reinforcement, however, be it directly confrontational or community shaming. Instead, norms are also internalized. Individuals pay attention to and internalize the opinions of others as a strategy to learn the nature of the games being played and to negotiate them effectively.³⁶ Internalizing

³² Random House Dictionary s.v. “gossip”.

³³ While gossip has indeed traditionally been dismissed as idle talk and otherwise diminished as a form of discourse (especially one linked with female communication), this position is increasingly being revisited and revised. See for examples: Daniel J. Solove, “The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure” (2003-4) 53 *Duke Law Journal* at 1044; Diane Zimmerman and Sally Engle Merry, “Rethinking Gossip and Scandal” in Daniel B. Klein ed., *Reputation: Studies in the Voluntary Elicitation of Good Conduct* (1997) 47 at 49.

³⁴ Daniel J. Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (New Haven: Yale University Press, 2007) at 84.

³⁵ Steven L. Nock, *The Costs of Privacy: Surveillance and Reputation in America*. (New York: Aldine de Gruyter, 1993) at 7.

³⁶ Daniel Klein & Jeremy Shearmur, “Good Conduct in the Great Society: Adam Smith and the Role of Reputation” in Daniel B. Klein ed., *Reputation: Studies in the Voluntary Elicitation of Good Conduct* (1997) 29 at 39. (referencing Goffman)

thus works as a form of enforcement without (active) shaming because “people not only want to avoid blame, but blameworthiness.”³⁷

Hart’s discussion of rules provides insight into the role of internalization. He makes a distinction between the “external” and “internal” aspect of rules; “[w]hen a social group has certain rules of conduct, this fact affords an opportunity for many closely related yet different kinds of assertion; for it is possible to be concerned with the rules, either merely as an observer who does not himself accept them, or as a member of the group which accepts and uses them as guides to conduct.”³⁸ In distinguishing these types of thinking, he uses the example of a red traffic light, suggesting that the external observer will understand only that the red light indicates a strong likelihood that traffic will stop, whereas the internal understanding of the red traffic light is not merely that it indicates a probability of traffic stopping but rather that it is a signal to individuals that they must stop. The difference between the external and internal perspective, then, is located in “the internal aspect of rules seen from their internal point of view” rather than in systems viewed from outside.³⁹ At least arguably, then, a norm which has not been internalized may indicate that a certain behaviour is expected, but once internalized the norm becomes instead that a certain behaviour is required and ought to be performed.

This is an interesting phenomenon in its turn, because internalization may result not only in individual norm-adherence, but in the individual who has internalized the norm(s) becoming in her turn a norm-enforcer; that is, that having bought in to the norm, the individual may also be (re)enforcing the norm by encouraging others to acknowledge and conform to it. This, in its turn, may have the effect of increasing group adherence to the norm – the more people who are enforcing the norm implicitly

³⁷ Daniel J. Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (New Haven: Yale University Press, 2007) at 99.

³⁸ H.L. A. Hart, *The Concept of Law* (Clarendon Press, 1961)

³⁹ *Ibid.*

or explicitly, the more likely it is that even those who have not internalized the norms will adhere to them in order to participate.⁴⁰

The choice of the term “participate” is a deliberate one – I will discuss more fully in chapter 4 the role of (good) reputation in granting access to services and community participation. As a precursor to that discussion, let me simply say that the assessment of an individual’s adherence to group norms functions not only to enforce adherence to those norms – instead, such assessments form the basis for many determinations, including commercial treatment, allocation of resources, and admission to various institutions.⁴¹

Those who adhere to mainstream group expectations (norms) will be granted the benefits of access to services and community participation by the mainstream, who adhere to those norms, while those who fail to meet that dominant expectation “will incur a form of disapproval that will lead them to be less trusted, liked and respected in the future.”⁴² Group censure is not only focussed on the individual rather than on the action, it is also not fixed in time but projects forward.⁴³

Norms, then, can be understood as social conventions that dictate expected behaviour, and adherence to them is to some degree obligatory on those who wish to participate effectively in the society around which they are centered.⁴⁴ Norm adherence as a precursor to effective participation comes because failure to model that adherence has

⁴⁰ Lawrence E. Mitchell, "Understanding Norms" (1999) 49 *University of Toronto Law Journal* at 217

⁴¹ Daniel Solove, "The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure" (*Duke Law Journal* 53 2003-4) at 1039

⁴² Cass Sunstein, "Group Judgements: Statistical Means, Deliberations, and Information Markets" (2006) 80 *New York University Law Review* at 985

⁴³ When I say “mainstream group expectations” this should not be taken to mean that the group itself is or must be mainstream. Rather, I refer to the prevailing expectations of whatever group is at issue at the time. This may and almost certainly does place the individual in a state of constant conflicting expectations depending on how many groups s/he interacts with, but for the purposes of this discussion, it is the assessing group whose expectations are at issue and to which conformance is judged.

⁴⁴ Lawrence E. Mitchell, "Understanding Norms." *University of Toronto Law Journal* 49 (1999) at 182.

repercussions. This in turn happens because “conformity to group standards is necessary to earn a good reputation. A bad reputation is usually the product of having been shamed. And there are powerful incentives to avoid shame because, once shamed, there are few ways to absolve the bad reputation.”⁴⁵

Norms and the Derivation of Reputation

The role of reputation is inherently public – that is, while image is self-directed, reputation is by definition other-directed and derived;⁴⁶ further it is derived for the purpose of functioning as a kind of social lubricant – to facilitate relationships among persons by reducing uncertainty and thus helping to create trust.⁴⁷ Even where “trust” is not created, reputation may function to simplify the complexity of everyday interactions by providing people with a superficially justifiable reason for behaving a certain way in relation to others based upon their “reputation” either as an individual or as a member of a group, based on the presumptively predictive value of reputation.⁴⁸ Unsurprisingly, then, reputation has achieved ever greater importance and utility as the opportunity(s) for uncertainty have increased.

In the discussion of norms, I examined how an individual may be cast as “good” or “bad” based on their adherence to and modelling of social norms; this positioning is the assigning of reputation based on norm adherence. In this way reputation may be said to be comprised of signals as interpreted by others. At the same time, however, reputation has come to function as a signal in and of itself.

⁴⁵Steven L. Nock, *The Costs of Privacy: Surveillance and Reputation in America*. (New York: Aldine de Gruyter, 1993) at 2

⁴⁶ Rosaria Conte and Mario Paolucci, "Reputation in Artificial Societies: Social Beliefs for Social Order." In *Multiagent Systems, Artificial Societies, and Simulated Organizations*, edited by Gerhard Weiss,(2002) at 71.

⁴⁷ Steven L. Nock, *The Costs of Privacy: Surveillance and Reputation in America*. (New York: Aldine de Gruyter, 1993) at 124

⁴⁸ Steven L. Nock, *The Costs of Privacy: Surveillance and Reputation in America*. (New York: Aldine de Gruyter, 1993) at 124

Preliminary Exploration of Trust

In order to make the claim that 'appropriate' internalization and modelling of norms will lead to trust, it is necessary to interrogate what "trust" actually encompasses.

The concept of trust has been explored in a variety of disciplines and from a variety of perspectives: where psychology looks at trust from an individual aspect, social sciences position it more as a reflection or product of community social processes and interactions. Economic analysis tends to explore trust instead from an organizational viewpoint, examining economic rather than interpersonal implications.⁴⁹ My project, however, is concerned with mapping the intersections of individual and social processes, recognizing an inherent organizational and economic aspect contained within, and resulting from, the trust analysis. As such, it is necessary to synthesize the various academic perspectives in order to attempt to formulate an understanding of trust that is sufficient for my purposes.

In their exploration of trust, Mayer et al. provide a strong analysis of what trust is not. For them, trust is necessarily something more than mere co-operation (since people may work together towards a common goal without trusting each other)⁵⁰ or even predictability (because the ability to predict someone's behaviour or outcome does not necessarily lead to a willingness to undertake risk).⁵¹ Mayer et al. focus on the willingness to make oneself vulnerable; to expose oneself to risk. This decision is necessarily an informed one, and this is the final distinction made, between confidence and trust, where confidence indicates a state of faith rather than the product of a risk analysis.⁵²

⁴⁹Rajeev Bhattacharya, Timothy M Devinney & Madan M Pillutla, "A Formal Model of Trust based on Outcomes" (1998) 23:3 The Academy of Management Review ; ABI/INFORM Global pg. 459 at 460.

⁵⁰Roger Mayer, James H Davis & David F Schoorman, "An Integration Model of Organizational Trust" (1995) 20:3 The Academy of Management Review ; ABI/INFORM Global, 709 at 712.

⁵¹ *Ibid.*

⁵² *Ibid.*

As Mayer et al. position trust, it is integrally linked not only to risk analysis but also to risk-assuming behaviour. That is, the level of risk one is willing to assume will be determined by the amount of trust that is held. That amount of trust held is not fixed but is a product of the context and players in which the analysis takes place. In each situation, then, trust and risk analysis are key factors in the decision about whether and how much risk to assume in entering into a given transaction.⁵³

Where trust analysis may be focussed on a discrete transaction, it may also form part of a longer-term relationship and thus may not only factor into the development of reputation but may in turn then incorporate an assessment of reputation into future risk analysis. This is because just as trust includes a process of risk analysis prior to undertaking risk, so too will the results of that risk assumption ultimately become signals for future risk and trust analyses.

If part of trust is based on a risk analysis that incorporates knowledge of past behaviour, then a reputation for “good conduct” will be based on a history of good conduct that is thought to indicate a propensity for good conduct in future transactions.

Extensions of Reputation and Trust

Unfortunately, larger and increasingly dispersed communities make it increasingly unlikely for there to have been past transactions between the parties.⁵⁴ Potentially, where there is only a series of individual transactions with different partners, it is possible for the information gleaned by each individual in her separate transaction to be shared with others in the community. That is, when people have no history of past interactions with an individual upon which to depend, they begin to consult with

⁵³ “Transaction” is normally presumed to indicate an economic or commercial interaction, but the term is used here more expansively to include individual interactions and social relations as well.

⁵⁴ Daniel Klein & Jeremy Shearmur, “Good Conduct in the Great Society: Adam Smith and the Role of Reputation.” In *Reputation: Studies in the Voluntary Elicitation of Good Conduct*, edited by Daniel B. Klein, 29 (1997) at 37.

others, and this consultation provides them with information upon which to base a their trust and risk analyses and concurrent assumption of risk.

This sharing of information is also key to understanding the scope of information collection at this stage. If information is necessary in order to make a trust assessment, then it appears to follow that the more information that is available, the more reliable the trust assessment will be. A cycle of sorts is created and perpetuated by this process, where an individual must actively participate with others in the community – individual social relationships, commercial and non-commercial transactions between the individual and organizations – in order to be assessed by other community members.⁵⁵ From this assessment is derived a multiplicity of reputation assessments that may coalesce into a cumulative reputation while continuing to function independently in various situations where they are particularly relevant.⁵⁶ This reputation(s) in turn becomes important to future participation, which will lead to further assessment, a more in-depth reputation assessment, and thus future access. Each member of the community, then, is necessarily involved in a tripod of activities – individual performances, assessments of the performance of others, and transmission and collection of those assessments to others within the community.

In the absence of such information sharing, there is also a move toward the development of proxies such as credentials and ordeals. A credential is a token of trust⁵⁷ such as a signature, a personal identification number or other ‘official’ verifications in the forms of educational degrees or driver’s licenses. An ordeal, in contrast, is something like an integrity test or even a lie-detector or drug-test.⁵⁸ Such

⁵⁵ It should be noted that despite participation, the collection of information may not translate into increased reliability where the information is inaccurate or even where there is so much of the information that it’s unable to be processed in any useful or meaningful way.

⁵⁶ Given that identity performances as well as transactional performances are inherently context-specific, it follows that at least some reputations or aspects of reputation will also be context-dependent.

⁵⁷ David Lyon, *Surveillance Society* (McGraw-Hill, 2001) at 15

⁵⁸ Steven L. Nock, *The Costs of Privacy: Surveillance and Reputation in America*. (New York: Aldine de Gruyter, 1993) at 11

proxies function as authentication of the individual or some quality of the individual in the context of integrity tests etc., but do not provide the extensive details that community knowledge can provide. Indeed, such proxies confirm the identity or (presumptive) truthfulness of an individual but still leave open the question of how to make an assessment of trustworthiness of that authenticated individual. As Steven Nock writes:

When I make a purchase, for example, I do so from strangers, who need some token to show that I can be trusted and have the resources to pay. But this raises acutely the question of who can be trusted if the stranger – or the institution – has not had the opportunity personally to check the reputations, credentials and credibility of those with whom they must nonetheless interact day to day.⁵⁹

Nock concedes that such proxies do not provide much substantive information, but he argues that this is not necessarily an issue and that extensive information is unnecessary – rather, what is needed is “a simple distinction between those who do and who do not play by the same rules.”⁶⁰

If what is needed can be reduced to the ability to discern whether someone does or does not “play by the same rules”, then I can return to the idea of reputation – it is in this way that reputation becomes a signal itself.

Reputation as Proxy for Trust

The discussion of norms, trust and reputation has thus far focussed on co-present relationships. Traditionally, communities were small and localized, resulting in a situation where participants in a relationship were likely to know each other and thus

⁵⁹ Steven Nock, cited in Lyon, *Surveillance Society*, supra note 56 at 21

⁶⁰ Steven L. Nock, *The Costs of Privacy: Surveillance and Reputation in America*. (New York: Aldine de Gruyter, 1993) at 73

there was little uncertainty felt or likely to be felt.⁶¹ Even where participants might not directly be acquainted, small communities meant that each individual's social and kinship connections were known to some degree, and so although technically a stranger, the individual was still "known" in some fashion that reduced uncertainty. Indeed, not only would the individual be "known", but as a member of a shared community the degree of their adherence to a set of recognizable norms could be predicted, at least presumptively. This, in turn, creates the possibility of making a trust assessment, and said assessments shape the degree of willingness to assume the risk of entering into a transaction or relationship with the other. That is, the unknown is a status of great risk. The more known something or someone is, the less risky the transaction may appear. Similarly, even where unknown, shared norms, or reports that indicate the degree of adherence to shared norms, are also held to contain information that lessens the risk of the complete unknown and thus of entering into a transaction with that person.

As discussed previously, trust is a multi-faceted term with a variety of focuses and meanings. Attempting to synthesize the various perspectives around trust leads us to a definition of trust as "the expectancy of positive (or non-negative) outcomes that one can receive based on the expected action of another party in an interaction characterized by uncertainty."⁶² Essentially, trust underpins a willingness to assume risk based on an analysis that indicates that the trustworthiness of the situation and player outweighs the risk of the situation and player.

As societies progressed and became more complex and more dispersed, it became less possible to rely on co-presence and extended relationships, and the resulting uncertainty made trust became more difficult. The lack of co-presence did not

⁶¹ Of course, the belief that someone is "known" does not necessarily mean they are intimately familiar with them. Rather, the sense of "knowing" comes from a presumption of shared points of reference – that we come from the same place, I know of you, I know of your family.

⁶² Rajeev Bhattacharya, Timothy M Devinney & Madan M Pillutla. "A Formal Model of Trust Based on Outcomes." *The Academy of Management Review* 23, no. 3 (1998) at 462

correspondingly decrease the need to make such assessments – if anything, it increased it. Accordingly, it is as societies moved towards larger, more dispersed groups, that proxies needed to be developed to allow for trust.

In the previous section I explored reputation as a marker of adherence to mainstream social group norms, as well as the way that successful risk assumption may itself lead to the development of a positive reputation. It is easy to see, therefore, how reputation can be effective as a proxy for trust. Familiarity, similarity and shared values may all function as triggers of trust⁶³, and reputation contains this information within it. For members of a homogenous small community, it models the small community knowledge and enforcement with which all are familiar and functions as indicia of shared values and norms.⁶⁴

The Role of Trust

Trust may have a larger dimension as well; Nissenbaum extends the definition, speaking of trust not as individual belief but rather as “the expectation that arises within a community of regular, honest and cooperative behaviour, based on commonly shared norms, on the part of other members of that community.”⁶⁵

Everyone is familiar with the way(s) in which trust nuances relationships – among trusted friends or family we are able to freely joke, speak bluntly, take verbal short-cuts, speak on contentious subjects, or even be comfortably silent⁶⁶ – all things that would be extremely risky in the company of those less-known and trusted.

⁶³ Helen Nissenbaum, "Securing Trust Online: Wisdom or Oxymoron?", (2001) 81 B.U.L.Rev. at 644

⁶⁴ Of course, just as within those small homogenous communities, those who fall outside the mainstream by reason of sex, gender presentation, race, class, ability or a variety of other characteristics will have more limited access based on a separateness from those co-extensive norms.

⁶⁵ Helen Nissenbaum, "Securing Trust Online: Wisdom or Oxymoron?", (2001) 81 B.U.L.Rev. at 644

⁶⁶ *Ibid.*

Reputation is a key element of trust – one that may be said to function as “a kind of social credit, a form of currency”⁶⁷ that purchases or at least facilitates trust in relationships where personal knowledge is insufficient. It does so by conflating information collection with knowledge – that is, there is a belief that knowledge will allow us to predict the behaviour of those with whom I interact,⁶⁸ and if I can predict behaviour then I will be able to manage risk appropriately. Accordingly, the belief is that the more information we know, the more reliable our assessment(s) will be and thus the greater our ability to trust.

The Goal of Trust

Nissenbaum has identified four (4) elements that affect the readiness to extend trust: publicity/publicness; a system of reward and punishment; the promulgation of norms by means other than reward; and where possible, some form of trust insurance.⁶⁹

When Nissenbaum speaks of publicness, she invokes the idea of the spotlight – that is, the idea that people are more willing to extend trust in a system where actions are public and visible rather than obscured or hidden. The publicness of reputation is clear – reputation is assigned by others, and is derived through interactions with others. Reputation is by its very nature a public process.

Reward and punishment too are inherent in reputation – where shaming is punishment for failure to adhere to norms, a ‘good’ reputation and social lubrication are the rewards for being perceived to do so.

Being part and parcel of a system of norm adherence and assessment, reputation also meets the third requirement. Norms are enforced not only through the active rewards

⁶⁷ Lawrence M. Friedman, *Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety and Privacy*. (Stanford: Stanford University Press, 2007) at 27

⁶⁸ Julie E. Cohen, "Privacy, Ideology and Technology: A Response to Jeffrey Rosen" (2000-2001) 89 Geo.L.J. at 2031

⁶⁹ Helen Nissenbaum, "Securing Trust Online: Wisdom or Oxymoron?" *B.U.L.Rev.* 81 (2001) at 646

and punishments of shaming and reputation derivation, but also are reinforced through their effect; that is, a 'good' reputation carries with it the reward of access to desired services and knowledge. It also carries with it effective community participation, while a 'bad' reputation may increase the cost and difficulty of participation, may bar access entirely to a particular transaction, or even to an entire sphere of transactions or interactions.

Alas, reputation does not carry within it any form of trust insurance. However, it is interesting to note that while Nock argues that "reputation earns trust"⁷⁰, Nissenbaum has made the suggestion that rather than extending trust based on reputation, trustees actually "form expectations regarding the likely actions of these others."⁷¹ Intuitively, this makes sense. I have discussed norms as a set of social expectations that dictate expected behaviour, and a person's reputation as a signal that they have been found to meet the norms of those with whom they have interacted. If indeed trust is a willingness to enter into a transaction (or not) based on the belief that the other will behave in the way expected, then reputation cannot stand in for that belief – it can only furnish the information upon which a risk assessment can be based. Trust, then, may be said not to be earned by reputation, but rather to be based on a risk-assessment informed by reputation. As such, there may be no trust insurance, but prior to extending trust individuals are able to make a full risk-assessment based on information beyond their own experiences, and as such some form of predictability, if not insurance, may be said to exist.

Extending Trust to Online Spaces

Steven Nock's book focussed on what he called "the emancipated", that is, young people who, due to changes in social and economic spheres, no longer remained within their community but struck out on their own. Lacking the community trust-markers, new

⁷⁰ Steven L. Nock, *The Costs of Privacy: Surveillance and Reputation in America*. (New York: Aldine de Gruyter, 1993) at 44

⁷¹ Helen Nissenbaum, "Securing Trust Online: Wisdom or Oxymoron?" *B.U.L.Rev.* 81 (2001) at 644

trust processes needed to be developed to deal with this situation in order to allow individuals to interact effectively in a culture of strangers.

There is reason to believe that the development and increasing pervasiveness of online environments creates a situation akin to the emancipation on which Nock focussed; in online environments people interact with strangers who are unknown to them and unauthenticated. It is, therefore, an environment that simultaneously requires trust assessment and yet provides none of the markers with which we are traditionally familiar in order to make those assessments.

As Nissenbaum recognizes:

Trust is a key to the promise the online world holds for great and diverse benefits to humanity...people shy away from territories they distrust; even when they are prepared to engage voluntarily, they stay only as briefly as possible. Without people, without participants, many of the visions will be both literally and figuratively empty. Trust would invigorate the online world; suspicion and insecurity would sap its vibrancy and vitality.⁷²

The online environment, then, requires trust even as it defeats the kind of informal information sharing that enables the risk-assessment upon which trust is traditionally based. Nissenbaum critiques the presumption that security measures can ground trust, arguing that a focus on security not only doesn't meet the needs of trust, but in fact misconstrues its roots.⁷³

Surveillance

Nock suggests that surveillance is the response to the emancipated; I want to suggest that when I discuss trust in online spaces, I am talking about an analogous situation, that just as the "emancipated" were unknowns and surveillance evolved to meet the

⁷² Helen Nissenbaum, "Securing Trust Online: Wisdom or Oxymoron?", (2001) 81 B.U.L.Rev. at 644

⁷³ *Ibid.*

need to attach information to strangers in order to facilitate risk-assessment, so too do reputation systems in online spaces function as a form of surveillance whose intent is to make hitherto obscured individuals “knowable” in ways that can facilitate trust.

Discourse around surveillance has tended to focus on the way(s) in which technology facilitates ever-greater (and increasingly fragmented) surveillance of individuals. Although it is true that the systematization of reputation into an aggregate and ongoing assessment is technology-based, the intent of this chapter is not to focus (as so many have already ably done) on the role of technology in perpetuating and increasing surveillance.

The term “surveillance” is derived from the French “sur” meaning over, and “veillance”, meaning to watch. At its most basic then, surveillance means to watch over. Dictionary definitions include “oversight; watch; inspection; supervision.”⁷⁴ To watch “over”, especially when understood in terms of oversight or supervision, implies something beyond mere viewing – it implies a watching from above of those below. Giddens has distinguished two types of surveillance; one is “gathering information on” and the other is “supervising.”⁷⁵ In both cases, however, the implication of watching from above of those below is retained.⁷⁶

I have already discussed the way norms, reputation and trust become interdependent, especially in an increasingly distanced society. Similarly, surveillance does not exist in isolation, but is rather the social outgrowth of an (increasingly) administrative system. Lyon notes that, “in modern societies, the use of forcible methods to keep social control

⁷⁴ Webster's Revised Unabridged Dictionary. s.v. "Surveillance". n.d.

⁷⁵ David Lyon, *The Electronic Eye* (University of Minnesota Press, 1994) at 11

⁷⁶ My intent is to suggest that reputation systems in online spaces are often created and instituted for the purpose of “supervising” – of exercising control over users via watching. But in actual fact, they function instead as a facilitator of “collecting information on” – that is, that not only does the site collect information about its users, but that the mechanisms of reputation systems enable users of the site to collect and provide information about each other.

has diminished drastically, replaced by administrative control (keeping tabs) and by new systems of codified law and policing.”⁷⁷

I want to focus now on the ways that surveillance and reputation seem inextricably linked. Reputation and trust achieved increasing interdependence as knowledge and community expanded beyond co-presence. David Lyon makes a similar point about surveillance, noting that historically relationships have been one-to-one and embodied, with co-presence creating trust as people are able to rely on their own assessments of the other.⁷⁸ As societies become increasingly complex and more dispersed, however, it becomes less possible to rely on co-presence for the derivation of assessments, and thus co-presence began to give way to other markers of trust.

Modes of interaction began to alter radically in modern times, as transport and communication allowed people to be more mobile, and social institutions helped to mediate their relationships. So the signature, for instance, became more important as a guarantee of legitimate identity and was accepted by organizations such as banks. These organizations extended the range of human actions, as did artefacts such as the telephone, so that more and more could be done at a distance without the co-presence of bodies in relation. A token of trust, such as a personal identification number, became a proxy for the kind of trust that arises from an ongoing relationship of co-present persons.⁷⁹

Just as the waning of co-presence was perceived to require the development of proxies⁸⁰, so too does the increasingly anonymous (and anonymized) urban technological culture necessitate some new form of reputation assessment.

As Lyon remarks:

⁷⁷David Lyon, *The Electronic Eye* (University of Minnesota Press, 1994) at 103

⁷⁸David Lyon, *Surveillance Society* (McGraw-Hill, 2001) at 15

⁷⁹*Ibid.*

⁸⁰Of course, whether this is actually the case is another thing. Although people believe that co-presence allows them to “know” someone, there may actually be legitimate questions about the degree to which co-presence is actually informative in the way they believe.

Since the 1960s, bodies have been disappearing at an accelerating rate. Communication and information technologies enable not only fax and fixed phone communication, but also email, credit card transactions, cellphones and the Internet. This means that many other relationships become possible without co-presence. Bodies and personal experience part company, and a significant portion of that personal experience is social. The ties that bind are not electronic cables or satellite signals themselves, but they are increasingly mediated by electronic means. As the spread of such relationships picks up speed, so too does the quest for substitutes for traditional modes of integration.⁸¹

In this quest for substitutes, attention is increasingly being paid to the role of reputation in trust-derivation and in behavioural (re)enforcement. As Conte & Paolucci note:

In the ICT field, the interest in reputation has been growing rapidly during the past few years, especially under the impetus of a need for regulation of the services offered on communication networks. Matters of security, privacy, conflicts of interests and contract fulfilment, felt particularly in the domain of electronic commerce, require the establishment of conventions. However, the enforcement of conventions poses interesting problems to designers and scientists: how can they work in a domain where sanctions are hard to implement? In this light, reputation-based systems are seen as a distributed mechanism of enforcement.⁸²

There can be (and are) many different forms of reputation-based systems, and it would be a mistake to assume that all of them mirror the reputation processes previously discussed. Certainly some can be said to do so, being a system that creates and relies upon an aggregate of risk assessments within a single community. Others however, may not aggregate reputation, may operate across communities, or may even be informal networks of social interaction that rely on reputation and status informally.

⁸¹ David Lyon, *Surveillance Society* (McGraw-Hill, 2001) at 15

⁸² Rosaria Conte and Mario Paolucci, "Reputation in Artificial Societies: Social Beliefs for Social Order." In *Multiagent Systems, Artificial Societies, and Simulated Organizations*, edited by Gerhard Weiss,(2002) at 30.

Nevertheless, the point remains that the recognition of the efficacy of community regulation offline via reputation has resulted in an interest in reputation-based systems as a form of enforcement and community regulation.

Conclusion

Social norms and the adherence to and modelling of them are acknowledged indicia of being viewed positively – that is, if failure to adhere to the norms results in discipline via ostracizing or othering, then successful internalization and adherence will be a key feature in achieving a positive light. As previously discussed, successful internalization and adherence are not the only features; deviations in class, gender, racialization and other grounds that inherently separate an individual from the mainstream and thus from the mainstream norms may act as their own barriers to the attainment of mainstream approval.

Similarly, trust has been shown to be the product of risk assessment that leads to a willingness to assume risk.

Information is integral to both of these processes. Without information, how am I to assess whether norms are being appropriately adhered to? And without information, how may an effective risk assessment be undertaken, sufficient to ground trust?

If trust does not depend upon being assured by others, but rather is derived from the ability to collect information and make one's own risk-assessment, then measures aimed at security cannot provide the desired certainty.

Nock identified surveillance as the response to an increasing number of stranger interactions, and argued that the use of overt forms of trust-markers (credentials and ordeals) facilitated the development of reputation upon which trust could be built.

Nissenbaum dismisses surveillance as one of the inefficient security responses⁸³, but I believe this inconsistency stems from different focusses on what surveillance might mean and how it could operate to facilitate trust. Certainly surveillance whose intention is to ensure that people behave may not provide the required information. But what about surveillance in a more visible and transparent way, that is, what about surveillance that not only watches participants in order to enforce desired behaviour, but does so visibly and transparently, so that other participants in the environment are able to collect information from it upon which to base their own risk-assessments?

Conte & Paolucci have noted that “rather than being reputation based, most of the classic systems accessible online track the results of agents’ personal experiences.”⁸⁴ This too springs from an understanding of surveillance that fails to consider how publicness and transparency of such systems might move personal experience into the realm of reputation and in so doing seek to enable trust based on risk-assessment. In the next chapter, I will consider such systemic surveillance systems to examine how they enable reputation derivation and risk-assessment.

⁸³ Helen Nissenbaum, "Securing Trust Online: Wisdom or Oxymoron?" *B.U.L.Rev.* 81 (2001) at 649

⁸⁴ Rosaria Conte and Mario Paolucci, "Reputation in Artificial Societies: Social Beliefs for Social Order." In *Multiagent Systems, Artificial Societies, and Simulated Organizations*, edited by Gerhard Weiss,(2002) at 194.

CHAPTER 2: Creation, Embedding and (re)Enforcement of Community Norms via Reputation Systems

Trust then is the product of an individual risk-assessment based on all available information. Reputation, in turn, functions not as a proxy for trust, but rather as a source or indicator – that is, reputation is information that individuals are able to incorporate into their own risk-assessment processes.

This is an important distinction, especially as I progress to examining the role that reputation is being asked to play in current online spaces, as well as the role it is actually playing. In order to do so, this chapter will interrogate the impact(s) of the use of reputation in online spaces and, in so doing, of systematizing reputation generally.

I intend to set out, in the following sections, the argument that reputation systems in online spaces function as a form of surveillance, and furthermore that through their imposition they exert a regulating force which, in turn, has a normative effect. What these norms are and how they are reinforced is further complicated, in reputation systems, by the use of lateral surveillance mechanisms to derive the base assessments from which the overarching reputation is derived. This chapter will seek to interrogate the tensions that arise between systemic messages and cultural messages in a lateral surveillance system; the disconnect between the role that reputation is asked to play and the role it is actually playing.

Discussion of the way that norms are imposed and reinforced by surveillance has tended to focus on the panoptic effect of surveillance.

In the first part of the chapter, I will set out the argument, to my knowledge not previously made in the existing literature in surveillance studies, that the institution of

a reputation system on a particular site or community can be a form of surveillance that is intended to have panoptic force.

Not all norms, however, are received “from above.” In the second part of the chapter, I make the argument that, in addition to the chosen norms which reputation systems are designed to (re)enforce, a second set of norms is also operated, these ones synoptically derived.

Finally, I will make the argument that in reputation systems where panoptic and synoptic norms become collapsed in this way a hybrid surveillant force is created, one that I term “transoptic”.

Participatory Surveillance

The difficulty of establishing trust through security measures has been addressed in chapter 1, which also provided some discussion of the role of reputation in reinforcing social norms and those same social norms in regulating/shaping behaviour. That is, performing behaviour that is consistent with mainstream norms gains positive reinforcement externally as well as the performance acting to reinforce those norms. Reputation systems that are based not only on surveillance but on participatory surveillance attempt to build on the distributed nature of social norms, as well as their effectiveness in behaviour controls.

Mark Andrejevic has postulated the development of a culture of scepticism where individuals have become too sophisticated (and perhaps too cynical) to easily trust disembodied trust markers. He links this scepticism to the move towards systems of participatory trust-marker development: “the injunction not to trust in discredited social institutions and traditional practices but to take matters into one’s own hands...”⁸⁵

⁸⁵ Mark Andrejevic, "The Work of Watching Each Other" 2:4 Surveillance & Society 479 at 494

This scepticism about institutional trust markers has led to a search for a participatory form of trust creation – a way to translate the original one-to-one assessment of trustworthiness into the newly technologized and dispersed context. In essence, what is desired is a return to the original model of co-present trust development, but one that is mediated by technology.

Technologies have thus been developed and implemented that, first of all, facilitate the linkage of a particular identity with reviews/histories/comments of the community(s) in which s/he interacts, and then “make an ongoing assessment of that reputation.”⁸⁶ These reputation systems tend to be marketed as a positive means of harnessing the communicative power of the internet – they are said to facilitate social and commercial matching, encourage connections, harness technology and technologize word-of-mouth. Because they achieve this technologized community standard, they are increasingly also looked to as a potential way to create and facilitate trust – they are not “objective” trust markers but rather are systems in which I am able to participate and thus in which I can have some comfort about placing my trust. By placing faith in the systems, I am able to have faith in the information generated by it, information upon which I can then rely in turn in making my risk-assessments.

Ideally, the institution of such systems has a twofold effect, “drawing from a distributed pool of reputations has the potential to ease the search for opportunities, ideas, friendships, cultural goods, and high-quality services; hand in hand, pressure will increase for honest behaviour, competence and fulfilling subtle human needs.”⁸⁷ Many will think of eBay when they think of reputation systems, but in fact many other ill-known sites also have some variation of a reputation collection and dissemination system available. Amazon.com, for instance, does not rate performance on transactions, but does allow users of the site to submit reviews of materials available on

⁸⁶ Roger Dingledine, Michael J Freedom, David Molnar, David Parkes, and Paul Syverson. "Reputation" (2003). Online <http://freehaven.net/~arma/jean.html>

⁸⁷ Hassan Massum & Yi-Cheng Zhang. "Manifesto for the Reputation Society" First Monday 9 (2004)

Amazon.com, including those provided by third-party vendors. These reviews are, in turn, subject to reputation rankings – users of the site can indicate how helpful a particular review was, and a reviewer may rise to the rank of “top reviewer” based on the feedback of others.

Reviewer status thus comes to be understood as a predictor of the trustworthiness and reliability of the review itself. Slashdot.org has a similarly dynamic reputation system in place, where site users submit and review news items as well as actively reviewing the contributions of others. Users of the site are able to modify their settings to show only top-rated items, and top-rated authors acquire ‘karma points’ that increase the weight of their reviews and ratings.

Dellarocos writes:

Word-of-mouth networks constitute an ancient solution to a timeless problem of social organization: the elicitation of good conduct in communities of self-interested individuals who have short-term incentives to cheat one another. The historical appeal of these networks has been their power to induce cooperation without the need for costly enforcement institutions. Before the establishment of formal law and centralized systems of contract enforcement backed by the sovereign power of a state, most ancient and medieval communities relied on word of mouth as the primary enabler of economic and social activity, and many aspects of social and economic life still do so today.⁸⁸

Behaviour is shaped by these systems, then, because the systems create “rewards” for long-term behaviour that meets the expectations of the individual community within which the reputation is generated.

When reputation systems are fully implemented, a positive reputation becomes key to achieving access to productive communications or transactions within the sphere.

⁸⁸ C. Dellarocos, "The Digitization of Word of Mouth: Promise and Challenges of Online Feedback Mechanisms" (2003) 49:10 Management Science 1407 at 1409

Accordingly, the development and maintenance of a positive reputation achieves ever-greater importance. While any given individual may be tempted to take the short-term gain offered by failing to uphold her end of the transaction, the existence both of feedback and a system that attaches an ongoing assessment of reputation to the identity of that individual inclines her instead towards meeting the expectations of each individual transaction in order to create opportunities for future benefits through future transactions. These methods are analogous to the functions of gossip and shaming in enforcing and reproducing social norms; where gossip is a sharing of information that simultaneously seeds social norms; shaming; the risk of shaming; and the desire not to be shamed all act to enforce those norms. Reputation, then, acts to shape the behaviour of an individual towards long-term rewards, rather than short-term satisfaction, and thus fulfills not only a reporting function, but a supervisory one of sorts, and as such may be understood as a form of surveillance. .

Surveillance, of course, is traditionally understood to refer to a situation of active watcher and passive watched; all the agency/power is in the hands of the watcher. Even when the surveillant gaze and its attendant norms are internalized into self-surveillance, the power to define and enforce the norms still belongs to the watcher.⁸⁹ Albrechtlund has suggested an alternative understanding of surveillance that keys on its mutuality, arguing that participatory surveillance “...can also be empowering for the user, as the monitoring and registration facilitates new ways of constructing identity, meeting friends and colleagues, as well as socializing with strangers. This changes the role of the user from passive to active, since surveillance in this context offers opportunities to take action, seek information and communicate.”⁹⁰ As such, the participation of individuals in surveillance (their own and that of others within the system) need not be passive but can constitute an active part of the surveillance system, as I argue such participation does in the case of reputation.

⁸⁹ Anders Albrechtlund. Online Social Networking as Participatory Surveillance. In *First Monday*. Volume 13, Number 3 (3 March 2008).

⁹⁰ *Ibid.*

Mutuality need not automatically equate with (meaningful) empowerment, nor does it necessarily interrupt the fact that the ultimate power still rests with the over/authority. Andrejevic's writings on lateral surveillance seem to implicitly recognize this⁹¹. He argues persuasively that:

[t]hese techniques cannot be separated out from the regimes of governance associated with the productive management of the state, but serve as a mean [sic] for offloading some of the responsibilities of this management onto the populace, whose do-it-yourself monitoring practices reinforce and replicate the imperatives of security and productivity.⁹²

This recognition of offloading maps on to understanding the nuances of how reputation may function as a form of surveillance; that there may be two levels operating within reputation. On a ground level, assessments are made by individuals and the power is thus dispersed and peer-to-peer rather than top-down, however there is a higher level operating, since those assessments are made with reference to a global/community standard. Although deployed by individuals, therefore, reputation acts to reinforce the global/community standard, both as the norm of the community and for the individual(s) involved in the transaction and as such operates as a top-down power even when deployed through individual reputations.

When surveillance is broken up into two separate levels, as I have explored here, the door is open to further complexities, and it is my contention that both reputation-based systems in online spaces and the norms they purport to perpetuate are significantly more complex than they are ordinarily understood to be.

⁹¹ This is not Andrejevic's point, however I would argue that his claim that about the colonization of social norms that reflect market knowledge implicitly supports the idea that overarching expectations – those of the majority, the top, and the leaders in a market economy – are being referenced and reinforced in lateral surveillance practices.

⁹² Mark Andrejevic, "The Work of Watching Each Other." *Surveillance & Society* 2, no. 4: 479-97 at 487

When reputation systems are implemented, this doubled duality – the two levels upon which reputation is built and the two aspects of rules – creates a nexus which may result in very different understandings of what norms and standards are being rated and upheld. That is, that while the design and deployment of a reputation system on a particular site or community can be a form of surveillance intended to exert a supervisory force over particular behaviour, the individuals within that system may in fact be making assessments based on internal criteria that are distinct from the external intent of the system designers, and that in fact the collapse of these two forces into one reputation system creates a hybrid reputation with a transoptic force.

Reputation Systems as External Surveillant Force

Reputation systems are instituted in an attempt to create and facilitate trust among users of a particular site. Such systems function not simply to report on the behaviour of site users, but through their visibility and transparency are intended to exert a regulating force, encouraging “good” behaviour and punishing (through negative or lack of feedback) behaviour which deviates from the desired norm.

Panopticism

It is virtually impossible to discuss surveillance without invoking the image of Bentham’s Panopticon and the writings of Foucault on the subject.

The original “Panopticon” was a prison design created by Jeremy Bentham. The architectural design was grounded in Bentham’s realization that:

... the more constantly the persons to be inspected are under the eyes of the persons who should inspect them, the more perfectly will the purpose X of the establishment have been attained. Ideal perfection, if that were the object, would require that each person should actually be in that predicament, during every instant of time. This being impossible, the next thing to be wished for is, that, at

every instant, seeing reason to believe as much, and not being able to satisfy himself to the contrary, he should *conceive* himself to be so.⁹³

Thus, the major architectural strategy of Bentham's design "...incorporates a tower central to a circular building that is divided into cells, each cell extending the entire thickness of the building to allow inner and outer windows. The occupants of the cells are thus backlit, isolated from one another by walls, and subject to scrutiny both collectively and individually by an observer in the tower who remains unseen."⁹⁴ The design thus allows the central authority to observe (opticon) all (pan), thus creating the state of permanent visibility that Bentham deemed most beneficial.

Michel Foucault later built upon Bentham's notion of the Panopticon, seeing in it a metaphor for the exercise of power in modern societies. He explains that:

[I]t can in fact be integrated into any function (education, medical treatment, production, punishment); it can increase the effect of this function, by being linked closely with it; it can constitute a mixed mechanism in which relations of power (and of knowledge) may be precisely adjusted, in the smallest detail, to the processes that are to be supervised; it can establish a direct proportion between 'surplus power' and 'surplus production'. In short, it arranges things in such a way that the exercise of power is not added on from the outside, like a rigid, heavy constraint, to the functions it invests, but is so subtly present in them as to increase their efficiency by itself increasing its own points of contact. The panoptic mechanism is not simply a hinge, a point of exchange between a mechanism of power and a function; it is a way of making power relations function in a function, and of making a function function through these power relations.⁹⁵

As Lyon paraphrases:

⁹³ Jeremy Bentham, *The Panopticon Writings* by Mweran Bozovic (London: Verso, 1995) at Letter 1

⁹⁴ Ben F Barton & Marthalee S Barton, "Modes of PoWer in Technical and Professional Visuals" (1993) 7:1 *Journal of Business and Technical Communication* 138

⁹⁵ See Michel Foucault, *Discipline and Punish: The Birth of the Prison* (New York: Vintage Books, 1995)

...[m]odern societies have developed rational means of ordering society that effectively dispense with traditional methods like brutal public punishment. Rather than relying on external controls and constraints, modern social institutions employ a range of disciplinary practices which ensure that life continues in a regularized patterned way. From army drill to school uniforms, and from social welfare casework to the closely-scrutinized factory worker's task, the processes of modern social discipline are depicted in sharp relief...[and] people co-operate and collude with the means of control.⁹⁶

Traditionally, surveillance within the panopticon was enacted (and was intended) to impose and enforce chosen norms/rules/behaviours, as is perhaps to be expected within a prison environment. Its goal was the production of “docile bodies” – to remove the need for policing of behaviour via force, replacing it instead with the creation of a state of vulnerability induced by perpetual visibility (or the perception of perpetual visibility) that resulted in individual's self-policing their own behaviours towards the desired outcome.

In this paper, I speak of reputation as having a “panoptic effect” – by keying on effect I am signalling that I am particularly interested not in the act of watching or actively disciplining bodies but rather in the perpetual visibility that is induced by panopticism and the attendant impact on individual behaviour.

Is Reputation Panoptic?

Reputation then may itself be a form of surveillance, indeed, it may be viewed as a hybrid of Giddens' two types of surveillance, having aspects of both information collection and supervision embedded within it. There are multiple types of information gathering taking place. One gathers information about an individual or entity by transacting or interacting with them; information is produced when individuals submit their experiences to a central space where it can be seen by others; information is further gathered by those who consult reputation to derive a measure of

⁹⁶ David Lyon, *The Electronic Eye* (University of Minnesota Press, 1994) at 7

trustworthiness; and at still another level, these individual reputations are gathered together to form an aggregate reputation, be it by word of mouth within a community or mediated by technology within a formal or informal reputation system. At the same time, it must be admitted that the gathering together of information about reputation or trustworthiness will always have some kind of supervisory function. That is, awareness of the sharing of information should (and does) exert some kind of restrictive effect upon the behaviour of any individual who wishes to continue active (and productive) participation in that community. This can be said to be a form of social control.

The setting up of reputation systems on sites, however, also exists as (and exerts an) institutional control. This is because, first, the individual site must be recognized as an institution itself. As Lianos recognizes:

Institution is used here to indicate any source of mediating activity between human beings. In this sense, all private and public organizations and establishments are institutions because they regulate aspects of human behaviour as third parties i.e. without being subject to cultural negotiation. A super-market, a ministry and a web portal are all important sources of institutional sociality and normativity, and they should be understood, because of their combined effects on their users, as parts of the same regulating universe.⁹⁷

Of course, reputation systems are not institutional controls simply because they take place within an institution. Rather, they function (and should be recognized) as a form of institutional control because they are set up to support and facilitate particular kinds of desired performances, and to discourage behaviours which are not desired.

The power of this supervisory reputation system to instantiate particular kinds of behaviours, and to discourage others is the exertion of its panoptic force. By setting up the institutional framework, site administrators are able to shape

⁹⁷ Michalis Lianos, "Social Control After Foucault" (2003) 1:3 Surveillance & Society 412 at 413

behaviours – the act of operating within that framework transforms the regulation from one of sociality to an institutional one.⁹⁸

Recent writings on panopticism move away from preventing ‘bad’ behaviours and instead towards the regulation and instantiation of desired behaviours. Under such a model, surveillance is still present as a panoptic effect, but the move is (purportedly) towards the creation of access to benefits rather than the prevention of undesirable behaviours. This view of panopticism is primarily discussed in the context of consumerism⁹⁹, with the argument made that access to consumer consumption/participation functions as a reward, and the desire for reward itself shapes the behaviours of those who are subject to the system.¹⁰⁰

It should be noted, however, that the presentation of this as “reward” masks, to some extent, both the punishment and the manipulation inherent in the model. When a desire to participate crosses the line (even if only perceptually) into need, can I still talk about it as an uncomplicated reward? Or is there simultaneously a threatened withdrawal/denial of access as a punishment for failure to model the expected/desired behaviours?

Extending these ideas grounds my contention that reputation systems on sites exert a panoptic force – not necessarily by the imposition of discipline as to ‘correct’ behaviour (though that may indeed be the original intent) but rather because when possession of a ‘good’ reputation becomes the key to access to/participation on the site, individuals must adjust their behaviour/presentation accordingly in order to meaningfully access site resources.

⁹⁸ Michalis Lianos, "Social Control After Foucault" (2003) 1:3 *Surveillance & Society* 412 at 413

⁹⁹ See for example Haggerty & Ericson, "The Surveillant Assemblage" (2000) 51:4 *British Journal of Sociology* 605 at 615

¹⁰⁰ David Lyon, *The Electronic Eye* (University of Minnesota Press, 1994) at 61

Parsing Participatory Reputation Systems

It could, of course, be argued that since such a system is dependent for its efficacy on the voluntary participation of site users, oversight and control per se are not being exerted. Such an argument should, however, be dismissed on two counts.

First of all, the presumption of a separation between the participants of the system and the system itself is a fallacious one. Instead, it should be recognized that “in current conditions the majority of what one can call control does not focus on practices of constraint, nor on oppressing behaviour and expression, but on the organisation and the contextualisation of what is often intended or even desired by a sovereign subject.”¹⁰¹ To take the willingness of the site participants/community members to write themselves into the system, to shape it and to organize it such that the desires of the institution are therefore met is itself the exertion of institutional control. Indeed, the expectation of participation is inherent in online spaces and activities. As Andrejevic argues, “individuals are incited not just to participate in the forms of entertainment they consume (interactive television) and in the production of the goods and services they consume (mass customization), but in formerly centralized forms of surveillance and verification.”¹⁰²

Put another way, the decentralized form of surveillance which takes place on a site or community that implements a reputation system is an interesting one. On the one hand, the individual users are participating in a form of lateral surveillance, with peers watching peers, rather than an oversight body watching the many. On a more complex level, however, the norms that are being employed and reinforced through this veillance are still intended to be a product of the original surveillant panoptic force exerted by the reputation system design and implementation at the level of the institution. As Andrejevic puts it, “[i]nternalizing the gaze – in an era of governance of risk – comes to mean not just turning it upon oneself (in anticipation of the possibility

¹⁰¹ Michalis Lianos, "Social Control after Foucault" *Surveillance & Society* 1:3, 412-30 at 416

¹⁰² Mark Andrejevic, "The Work of Watching Each Other." *Surveillance & Society* 2, no. 4: 479-97, at 486

of being watched) but also directing it outwards towards others (as if to fill in the gaps of the big Other's gaze, to realize this gaze in a sceptical era) in the name of responsibility towards oneself."¹⁰³ Thus, the community here functions as an extension of the institution, and the surveillance in which they participate laterally perpetuates and enforces the norms set up by the original surveillance of the institution.

Finally, and perhaps even more importantly, the allegation that such participation is entirely voluntary and shaped by the users themselves must be interrogated. Technology, the space in which the system functions and the way(s) in which the system is implemented all have the power to shape the system. As Cohen notes, "information technology is not simply a passive conduit for pre-existing social values. The capabilities (and disabilities) of artifacts also shape social practices and priorities."¹⁰⁴

First, notice must also be taken of the role of the community in shaping information provision norms (as well as norms of behaviour). Writing about Facebook, Acquisti and Gross noted a seeming homogeneity in information revelation that existed across groups, and theorized that such homogeneity "may be the result of perceived peer pressure or herding behaviour."¹⁰⁵ Similarly, users who enter a site or community will receive participation and information provision as normalized within the site by virtue of existing user participation, and this normalization of information sharing enables their own uptake of the system. Arguably, users are particularly vulnerable to internalizing these norms due to the unfamiliarity of the space; where in our daily lives I understand the intended audience and the "tacit ground rules" for conduct in that

¹⁰³ Mark Andrejevic, "The Work of Watching Each Other." *Surveillance & Society* 2, no. 4: 479-97, at 486

¹⁰⁴ Julie E. Cohen, "Examined Lives: Informational Privacy and the Subject as Object." *Stanford Law Review* 52 (1999-2000) at 2036

¹⁰⁵ Alessandro Acquisti and Ralph Gross "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook,". *Proceedings of Privacy Enhancing Technologies Workshop (PET)*, Lecture Notes in Computer Science 4258, Springer, 36-58, 2006 at 10.

medium,¹⁰⁶ online spaces don't always come with such well-recognized expectations. Thus, the user is left to manage the "need to engage in 'normal' social behaviour, providing an account for one's actions in cyberspace as in any other social domain"¹⁰⁷ and thus is acutely aware of signals and expectations modelled in the community.

Second, it is important to consider that participation and its attendant provision/sharing of information is a "designed aspect of the system"¹⁰⁸; the (full) functionality of the system is dependent on users participating in it. Gary Marx has proposed the notion of mandatory volunteerism, "disingenuous communications that seek to create the impression that one is volunteering when that really isn't the case."¹⁰⁹ Such "volunteer" provision of information may take many forms; consent to security search before boarding an airplane, registration (and its attendant provision of personal information) as a precondition for using online sites and services, recording of telephone conversations purportedly for "quality assurance purposes" etc.¹¹⁰ In each case, the user is allegedly given the choice to consent to the collection of the information, but in actual fact the context in which the "request" is made is structured such that consent is the default response. Similarly, on such sites, although users purportedly have a "choice" as to whether to write themselves into the system by either reviewing or acting upon the reviews/reputations generated by others, in actual fact that choice is *de facto* made for them, since the only way to truly access the full functionality of the site is to participate within it.

¹⁰⁶ E. Wynn & J.E. Katz, "Hyperbole Over Cyberspace: Self-Presentation & Social Boundaries in Internet Home Pages and Discourse" *The Information Society* at 318

¹⁰⁷ *Ibid.*

¹⁰⁸ Adam N. Joinson "Looking at, looking up, or keeping up with people? Motives and use of Facebook" (SIGCHI 2008) 1027 at 1036

¹⁰⁹ Gary Marx, "Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information - 'Hey Buddy Can You Spare a DNA'" in T Monahan ed., *Surveillance and Security: Technological Politics and Power in Everyday Life* (London: Routledge, 2006) at 37.

¹¹⁰ Ian Kerr et al., "Soft Surveillance, Hard Consent" in *Lessons from the Identity Trail* (London: Oxford University Press, 2009) at 9.

There can be said to be, therefore, a dynamic interaction between surveillance and behaviour, where there is a conscious decision about what values are important and what results desired that impacts the technology.¹¹¹ Operating simultaneously, however, is another process – an unconscious prioritizing of certain values and the insertion of those values into the system by its participants.

While it would be a mistake to dismiss the surveillant force of reputation merely because it is carried out laterally by other users of the site, caution must also be taken not to deny any/all agency to the users of the site. Although the panopticon is often presumed to result not only in the regulation of behaviour but in the transformation of the desire to misbehave, concerns have been raised about the authenticity of such a transformation. Theorists argue that while norms may be internalized and applied, the individual will not necessarily transform into conformance with that norm, instead experiencing the “internal self-policing voice” as external to the true interior identity. In this way, it remains the exertion of an external force. This is consistent with Hart’s distinction between the external and internal aspects of rules – while the (externally imposed) panoptic system creates a strong probability that desired actions will take place (and undesired actions will not), the internal beliefs and standards of the system participants may be more nuanced than the rules set out by and for the external system and thus not fully accord with the external understanding of them.

It is my contention that while site administrators set out the parameters of reputation systems and the norms that the derived reputation will be used to uphold, site users may well be assessing reputation by reference to a set of norms derived not from site administration but from some larger reference point.

¹¹¹ Julie E. Cohen, "Examined Lives: Informational Privacy and the Subject as Object." *Stanford Law Review* 52 (1999-2000) at 2038

Synopticism

Thomas Mathieson has suggested the notion of a “synoptic” that has developed parallel to the panoptic.¹¹² Mathieson’s idea of the synoptic is not the superior few watching over the lower many, but rather involves a recognition that with the development and increasing permeation of mass media, we have also evolved a strong system of “the many watching the few” – that is, of the general population watching those in/on media. Mathieson sees both these “opticons” as endemic to our culture, arguing:

...[f]ormulated in bold terms, it is possible to say that not only panopticism, but also synopticism characterizes our society, and characterized the transition to modernity. The concept is composed of the Greek word *syn* which stands for together or at the same time, and *opticon*, which, again, has to do with the visual. It may be used to represent the situation where a large number focuses on something in common which is condensed. In other words, it may stand for the opposite of the situation where the few see the many. In a two-way and significant double sense of the word I thus live in a viewer society.¹¹³

In contrast to the externally imposed panoptic rules, the force of the synopticon is held to be much more effective in instantiating new beliefs/norms in the viewer. As Lyon writes, “mass media...can have a more direct effect on consciousness. It offers a world paradigm which fits current situations neatly, and is highly attractive to consumers who are positioned as ‘choosers’ rather than ‘creators’.”¹¹⁴

Of course, messages put forward by media may not be separate from those of the more formal governing and administrative institutions. The mass media is, as Chomsky has demonstrated¹¹⁵ inextricably interrelated with government and policy arms (especially

¹¹² Thomas Mathieson, "The Viewer Society" (1997) 1:2 *Theoretical Criminology* at 219

¹¹³ *Ibid.*

¹¹⁴ David Lyon, "9/11, Synopticon, and Scopophilia: Watching and Being Watched" in Kevin Haggerty & Richard Ericson eds., *The New Politics of Surveillance and Visibility* (Toronto: University of Toronto Press, 2006) 35 at 43.

¹¹⁵ Edward S Herman & Noam Chomsky, *Manufacturing Consent: The Political Economy of the Mass Media* (New York: Pantheon, 1983)

in the United States), and thus shares common interest(s) with them. As such, the synoptic message received from mass media may not differ appreciably from those promulgated panoptically.

Were it only traditional mass media, Lyon would be correct in warning that “[w]hile in principle everyone can indeed watch everyone else in mediated ways – screening the results – some forms of watching carry more weight than others.”¹¹⁶ However, I contend that not just the advent but the ever-increasing permeation of the internet may have undermined the messaging monopoly of mainstream media.

It would be glib to claim that the Internet or even the World Wide Web has completely democratized media. Certainly there remains a hierarchy of sites, where more corporate supported sites have greater permeation and greater accessibility. Nevertheless, the mainstream monopoly on media messages has been disrupted to some degree, especially in the web 2.0 environment. Time Magazine recognized this when, in 2006, they named “You” as the Person of the Year, writing:

You can learn more about how Americans live just by looking at the backgrounds of YouTube videos—those rumpled bedrooms and toy-strewn basement rec rooms—than you could from 1,000 hours of network television.

And we didn't just watch, we also worked. Like crazy. We made Facebook profiles and Second Life avatars and reviewed books at Amazon and recorded podcasts. We blogged about our candidates losing and wrote songs about getting dumped. We camcordered bombing runs and built open-source software.

America loves its solitary geniuses—its Einsteins, its Edisons, its Jobses—but those lonely dreamers may have to learn to play with others. Car companies are running open design contests. Reuters is carrying blog postings alongside its regular news feed. Microsoft is working overtime to fend off user-created Linux.

¹¹⁶ David Lyon, "9/11, Synopticon, and Scopophilia: Watching and Being Watched" in Kevin Haggerty & Richard Ericson eds., *The New Politics of Surveillance and Visibility* (Toronto: University of Toronto Press, 2006) at 48.

We're looking at an explosion of productivity and innovation, and it's just getting started, as millions of minds that would otherwise have drowned in obscurity get backhauled into the global intellectual economy.

Who are these people? Seriously, who actually sits down after a long day at work and says, I'm not going to watch *Lost* tonight. I'm going to turn on my computer and make a movie starring my pet iguana? I'm going to mash up 50 Cent's vocals with Queen's instrumentals? I'm going to blog about my state of mind or the state of the nation or the *steak-frites* at the new bistro down the street? Who has that time and that energy and that passion?

The answer is, you do. And for seizing the reins of the global media, for founding and framing the new digital democracy, for working for nothing and beating the pros at their own game, TIME's Person of the Year for 2006 is you.

Sure, it's a mistake to romanticize all this any more than is strictly necessary. Web 2.0 harnesses the stupidity of crowds as well as its wisdom. Some of the comments on YouTube make you weep for the future of humanity just for the spelling alone, never mind the obscenity and the naked hatred.

But that's what makes all this interesting. Web 2.0 is a massive social experiment, and like any experiment worth trying, it could fail. There's no road map for how an organism that's not a bacterium lives and works together on this planet in numbers in excess of 6 billion. But 2006 gave us some ideas. This is an opportunity to build a new kind of international understanding, not politician to politician, great man to great man, but citizen to citizen, person to person. It's a chance for people to look at a computer screen and really, genuinely wonder who's out there looking back at them.

Go on. Tell us you're not just a little bit curious.¹¹⁷

As *Time* recognizes, the disruption of mainstream control of messaging takes place in two ways – firstly, by making non-mainstream production of traditional media available to a greater audience and thus expanding their impact, but secondly by providing a platform upon which individuals may stand to raise their voices. As Ian Kerr notes, this platform functions in many ways:

¹¹⁷ Lev Grossman. "Time's Person of the Year: You". (Time Magazine, 2006)

...[n]etwork technologies fostered new social interactions of various sorts and provided unprecedented opportunities for individuals to share their thoughts and ideas en masse. Among other things, the Internet permitted robust political speech in hostile environments, allowing its users to say and do things that they might never have dared to say or do in places where their identity was more rigidly constrained by the relationships of power that bracket their experience of freedom. Anonymous browsers and messaging applications promoted frank discussions by employees in oppressive workplaces and created similar opportunities for others stifled by various forms of social stigma. Likewise, new cryptographic techniques promised to preserve personal privacy by empowering individuals to make careful and informed decisions about how, when, and with whom they would share their thoughts or their personal information.¹¹⁸

Synoptic Forces in Reputation

As discussed in chapter 1, awareness of and conformity to norms are inherent to any understanding of reputation. Nock explains that “through our dealings with others, an image is developed of the degree to which I do or do not conform to the standards that matter to them. Those who enjoy a ‘good’ reputation are thought to accept and abide by those standards – perhaps even demonstrating extraordinary conformance to them.”¹¹⁹

One might question how broad adherence to social standards and/or moral character can be deduced from an individual’s behaviour in an auction transaction, a book review, items one “Diggs” or any number of other activities upon which reputation purports to report. The short answer is that it cannot. That just as trust is not derived from reputation, but rather is derived from the ability make a risk-assessment based on relevant information, which will include reputation, so too must I distinguish behavioural signals from social responses to those signals. Thus, rather than being

¹¹⁸ Ian Kerr, "The Strange Return of Gyges' Ring: An Introduction" in *Lessons From the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* Oxford University Press, 2009 at xxiv.

¹¹⁹ Steven L. Nock, *The Costs of Privacy: Surveillance and Reputation in America*. (New York: Aldine de Gruyter, 1993) at 2

deduced from one's behaviour, the extent to which one does or does not conform to social norms may be extrapolated from successful interactions in the relevant spheres.

Vaz and Bruno describe the process as follows:

Although normalizing judgment can be understood as an infra-penalty that partitioned an area that the law had left empty – the vast domain of gestures, attitudes, quotidian activities, tasks, discourses, uses of time, habits, etc – its real novelty resides in the fact that these micro-penalties are not addressed so much at what one does, but at who one is. Besides constructing the dangerous bridge between fact and value and thus associating knowledge with power, the normalizing judgment also operates the passage from action to being, extracting from individuals' behaviour the identity of each and every one. The norm is an imminent law – an observed regularity and a proposed regulation.¹²⁰

Reputation systems, then, are comprised of a kind of lateral surveillance that incorporates both panoptic and synoptic processes, making possible a judgement of identity that extends beyond the rules/expectations of the particular site on which the transaction takes place. Individuals are asked, essentially, to rank the reputation of an individual with whom they have interacted or transacted in some way. Even though the system is designed to elicit feedback on designated aspects of the experience, all too often what is reported extends beyond that designed scope. If social norms are implicit in reputation, then reputation indicates the degree to which that individual conforms to the standards that are important to the reviewer – to “us”. What is assessed is the degree to which the individual is knowably ‘like us’ on the presumption that if I know what/who you are, I can then predict with some certainty whether you will act in ways that conform to the collective norms we have jointly constituted through previous interactions with others, both on the site and in general community.¹²¹ This means, then, that the actions of the individual on the site are not being rated in isolation as

¹²⁰ Paula Vaz & Fernanda Bruno, "Types of Self-Surveillance: From Abnormality to Individuals at Risk" 1:3 *Surveillance & Society* (2003) 272 at 277

¹²¹ Valerie Steeves personal communication (18 September 2012)

actions/transactions. Norms (including those internalized from mainstream media) outside the designed ones of the site come to the fore in the process wherein the reviewer measures the action of the individual against what they themselves would have done or expected in that situation. Individuals whose actions/responses match the norm-derived expectations of the reviewer will be thought of as “like me” and thus have overarching qualities of good moral character and social standard conformity ascribed to them. It is a correlative of this process that it is possible for an individual to meet every objective standard requirement for a particular transaction, yet fail to secure a ‘good’ reputation because while objectively their presentation was honest and trustworthy, the reviewer perceives them as having acted not as they themselves would, and thus finds them “not like I expected”. Unsurprisingly, since ‘like I expected’ results in the ascription of overarching positive qualifications and reputation, ‘not like I expected’ correspondingly results in ‘negative’ or at best ‘neutral’ or non-existent¹²² reputation.

Thus, although a reputation purports to be about an individual and is attached to the identity of that individual, in actual fact reputation may tell us more about the norms that are agreed to within a particular society than it does about the individual herself. Insofar as they tell us about that individual, it may well be a review of her ability to identify and conform to the social norm that is being assessed rather than her ‘self’ or even her objective performance of some task. It is my contention, therefore, that the norms against which conformance are measured are not wholly those set up in the institutional framework of the site, but rather that they are synoptically derived and thus culturally normative.¹²³ Ultimately, there may in fact be dual norms/processes at work.

¹²² The absence of reputation ranking may technically be considered simply “non-existent”, but I would argue that this is a misperception, since anything other than a positive ranking will tend to be read as negative in this binary culture.

¹²³ A word of caution; the community derived norms of which I speak are not explicitly those of mainstream media derived synoptically through viewing. Rather, that ongoing social interaction on the platform ultimately results in participants developing their own norms (as well as conforming and

EXAMPLE 1: COMMUNITY DERIVED NORMS: Ebay

The first and most obvious source of synoptically-derived norms may be the site users themselves. This group may function as a form of government in itself, and as such may develop its own norms and expectations. Certainly user-communities develop their own expectations of appropriate behaviour. No online denizen would expect the modes of conversation and participation which are perfectly acceptable on 4Chan¹²⁴ to be well-received on Cute Overload¹²⁵ or indeed (most) other sites.

Of course, neither 4Chan's /b/ community nor Cute Overload incorporates a reputation mechanism. To see how community-developed standards operate, let's consider eBay. eBay has a system where both the (registered) buyer and seller involved in a transaction are able to rate each other's performance,¹²⁶ and a cumulative feedback score of each individual is derived from the individual ratings received. As eBay explains, feedback "gives members a good idea of what to expect when dealing with other members."¹²⁷ Even non-eBay members are able to see the feedback score of a seller when they peruse the site, allowing them too to assess what to expect should they

reproducing the expectations built into the system). I link this to synopticism, however, because the norms that evolve through participation are also disseminated and adopted by other users through a process of viewing the norms in practice, internalizing and reproducing them. Thus, the many do take on the norms of the few participants as they become assimilated into site community.

¹²⁴ 4Chan's /b/ board are infamous and have been described as "A subset of 4chan, technically a "random image board," where completely anonymous — no login, no username — people try to shock, entertain, and coax free porn from each other. Encyclopedia Dramatica calls it the asshole of the Internet... Customs on /b/ include posts promising photos of personal degradation in return for certain kinds of porn or other helpful information; sarcastically asking for advice on teen romance; sarcastically asking/telling *anything*; pretending to have insider info or be privy to breaking news; posting image puzzles; and raiding other people's sites." Nick Douglas. "What The Hell Are 4Chan, ED, Something Awful and B?" (Gawker.com, 2008)

¹²⁵ A blog that features pictures of "cute" animals with accompanying "cute" vocabulary and commentary. The site refers to its denizens as "cuteologists" and has developed both Rules of Cuteness and its own "cutecabulary". See <<http://cuteoverload.com/>>

¹²⁶ Ratings are based on a five-star system and look at a number of factors, including accuracy of description, communication, shipping costs and speed of transaction.

¹²⁷ eBay. "Why Leave Feedback?" (How Feedback Works)

decide to enter into a transaction with this seller. In this way, individuals are able to draw from a pool of reputations and make their own assessment about trustworthiness in determining with whom they will enter into a transaction. At the same time, the existence of feedback acts to regulate behaviour – eBay puts this in terms of positive reinforcement, noting that “[l]eaving feedback is also a way to increase the goodwill of the eBay community by expressing your appreciation for a job well done. Finally, if you are a buyer, you can help spread the word about a seller you like, and if you are a seller, you can help recognize and reward loyal customers, which encourages them to buy from you again,”¹²⁸ but there is also a deterrent effect, where individuals are less likely to flout the rules or behave in untrustworthy ways when their behaviour will be permanently recorded and will impact on the availability of future transactions.

The eBay feedback mechanism is quite clear in its intention to report on the experience of individual transactions, yet I would argue that even within this seemingly delimited and defined reporting process, unspoken community-developed norms act to shape the perception of the other party to a transaction, and accordingly have an impact on reputation within the site.

Let us consider the relationship between speed of payment and online forms of payment, for instance PayPal. There is no formal requirement for buyers on eBay to use PayPal. Indeed, although some sellers do specify “PayPal only”, a quick perusal of auctions suggests that this is by no means the majority.¹²⁹ Nevertheless, reporting on speed of payment has come to enforce a presumptive norm of PayPal usage. Say, for example, that I bid on an auction and, upon winning it, immediately send payment through PayPal or a similar online payment system. When the seller rates our transaction as ‘positive’ or ‘neutral’, they also have the option of providing a comment to ground the review. Almost inevitably, one of the factors identified in these

¹²⁸ eBay. "Why Leave Feedback?" (How Feedback Works)

¹²⁹ Indeed, although eBay has changed its terms to mandate that PayPal be an optional method of payment for all auctions, there remains no requirement that PayPal be used by the buyer.

comments is speed of payment. So, having won the auction and paid immediately via an online payment service, the feedback I receive is likely to contain some kind of 'fast payer' reference, which is understood on the site as a recommendation. But consider an alternate situation, where I am a bidder in an auction. Aware that I am likely to be the winner, I am at the bank at auction close with my mobile and immediately on reception of the notification that I am the high bidder, I have a certified cheque issued to the seller and drop it into the mailbox. In both cases, money left my possession immediately upon close of auction and I am thus objectively an equally 'fast payer'. Yet in this second situation, although the seller can presumably determine from the date and time stamps on the certified cheque and envelope the immediacy of payment, this will not be recorded (nor, let's face it, even checked). Instead, there will either be a complete lack of reference to speed of payment or even the designation of me as a 'slow payer', something that is detrimental to my reputation on the site.

In this example, what operates to shape the review of my participation in the transaction is not in fact a review of my actual actions – rather, it is a review of whether I met the expectations of the individual seller. Further, those expectations of the individual seller constitute a community-developed norm against which my performance is measured and found lacking. This norm is not a function of eBay's architecture or regulation¹³⁰, nor is method of payment one of the behaviours that eBay's feedback system is set up to police – rather it is one that is community developed and that users of the community learn by viewing/watching the community. As such, this is a perfect example of a site reputation system which is designed to further one particular aim yet which in practice acts to enforce a community norm which is synoptically derived (rather than panoptically imposed) and yet functions to shape reputation.

¹³⁰ To be fair, however, as of October 2003 eBay has owned PayPal and thus while they do not mandate its use, their design and architecture provide multiple reasons not to forbid and perhaps even to encourage the institutionalization of this community-developed norm.

*EXAMPLE 2: MAINSTREAM NORMS: INTERNET DATING*¹³¹

A second form of this visible synoptic norm performance is at work in the assessment of reputation – one that comes not from the individual community in which the transaction takes place but rather from the mainstream society at large.

The *Love Online* report found in their survey of internet users that 89% of users were concerned that “people online might not tell you the truth about themselves” and 85% were concerned that “the people you meet online might be hiding something.”¹³² A Canadian survey from 2004 found that 80% of Canadians feel that online dating is dangerous because they don’t know whom they’re dealing with.¹³³ In order for online dating sites to be effective (and, not incidentally, commercially successful) these concerns must be addressed, and some sites have added some form of reputation system to their architecture in an attempt to mitigate such concerns.¹³⁴ Reputation systems in such circumstances, then, are intended to provide users of online dating sites with a feeling of security by allowing them to go beyond the inherently risky self-descriptions of users and rely instead on an online version of the offline word-of-mouth reference process¹³⁵ to find those who have accurately portrayed themselves.

I would argue, however, that in the community assessment that is conducted, reputation is being derived by determining not accuracy of self-presentation but rather acceptability of self-presentation, and further that acceptability/worthiness is a reflection of conformance to standards above and beyond (perhaps even unrelated to) accuracy and truthfulness in self-presentation.

¹³¹ Dating sites considered for this section were primarily targeted at heterosexual pairings.

¹³² Dr. Robert J. Brym & D. Rhonda L. Lenton. *Love Online: A report on digital dating in Canada*. (2001) funded by MSN. Toronto, online: <<http://projects.chass.utoronto.ca/brym/loveonline.pdf>>.

¹³³ Leger Marketing Report. *Canadians and Online Dating*. (2004), online: <<http://www.legermarketing.com/documents/SPCLM/040809ENG.pdf>>.

¹³⁴ Ellen Gamerman “The Undateables” *Wall St. Journal* (23 September 2006), online: <<http://online.wsj.com/article/SB115896346394071750.html>>.

¹³⁵ Mark Andrejevic, “The Work of Watching Each Other.” *Surveillance & Society* 2, no. 4: 479-97 at 490

The characteristics of the majority of users of online dating sites,¹³⁶ the nature of the transactions engaged in on the sites,¹³⁷ and ingrained power dynamics all contribute to defining the context in which interactions take place on the sites, and informing the reputation assessments performed on the site.

To understand the factors influencing reputation, dating sites should not, perhaps be thought of as “social networks” and instead be considered as inherently commercial sites. It is interesting to consider what is actually being “purchased” via membership to an online dating site. This is not social matching, where individuals are connected by a trusted third party based on self-reporting and reputation assessment, but rather a market wherein someone who has paid for the chance to acquire a date reviews the reputation of ‘sellers’ in order to evaluate the goods they have on offer.

Obviously, both men and women purchase memberships to dating sites. However, it appears that the fact that a majority of the users of the site are men, combined with a seeming asymmetry of self-worth¹³⁸ may have an influence on the standards to which conformity is expected. In such male-dominated spaces, as Stomblor argues, “in general, men develop the rules or scripts for both men’s and women’s interaction as gendered sexual beings. Men set the standards for interaction and valued behaviour

¹³⁶ The Love Online study found that “compared to Internet users in general, online daters are more likely to be male, single, divorced, employed in the paid labour force, and urban.” 2.

¹³⁷ Although online dating sites are generally free to browsers, there are inevitably fees involved with gaining access to information and features. Both membership and the ability to contact other members are generally available only to those who pay, either via a monthly fee or on a pay-per-use basis.

¹³⁸ A recent study discusses a male predisposition to presume members of the opposite sex are attracted to them, so that “men tend to misinterpret innocent friendliness as a sign that women are sexually interested in them...[while] there is an opposite bias in women’s errors. They tend to undervalue signs that a man is interested in a committed relationship.” “Don’t Misunderestimate Yourself: why people think that rivals are better looking than they really are ” *The Economist* 381:8505 (November 25, 2006) <<http://www.economist.com/node/8313758>> 84. Leaving aside both the heteronormativity of the study and the asymmetry of categories (sexual interest versus committed relationship), this is still an interesting point about self-worth.

and define femininity as (1) women's sexual attractiveness and availability to men and (2) women's sexuality in general."¹³⁹

Reputation on online dating sites may be developed from many activities – participation on site forums, private online interactions with other members, offline interaction with other members, profile review etc. To some extent, then, as with the eBay example I see the emergence of community-based norms; users of a particular site will need to actively participate in the site and do so in the expected/rewarded ways in order to receive positive reputation. My interest is in parsing that “expected” way, given the foregoing, it is perhaps unsurprising to note that although the system's original aim was to ascertain that people are who they say they are, good reputation on such sites appears to have much more to do with performance of the appropriate gendered characteristics. As such, an individual who posts an honest and correct profile and description of herself but does not meet mainstream gendered norms of attractiveness, presentation etc. may receive a low or nil reputation ranking. The norms of interaction that are applied in such situations appear not to be wholly site-community driven, but rather seem to conform to mainstream gender expectations beyond those on one particular site.

Michele White has noted how “Amazon's personalization options seem to allow spectators, who are depicted as active users, to write into the system and program it according to their desires.”¹⁴⁰ Similarly, reputation systems on online dating sites allow the male active users to program both the system (and, not incidentally, the women who participate within it) according to their desires and expectations. Thus, particular forms of masculinity are coded into the space itself and re-inscribed by the users, while particular forms of femininity are enforced by the context of the interactions.

¹³⁹ Mindy Stomble, "Buddies or Slutties: The Collective Sexual Reputation of Fraternity Little Sisters" (1993) 8:3 *Gender & Society* at 291

¹⁴⁰ Michele White, *The Body and The Screen: Theories of Internet Spectatorship* (Cambridge: MIT Press, 2006) at 24

Reputation in online dating sites, then, is a form of co-veillance whereby the community applies synoptically derived norms to the derivation of reputation, thus incorporating and ultimately enforcing the synoptic norm.

EXAMPLE 3: USER DETERMINED CONTENT: DIGG

In previous examples, there has been some tension (acknowledged or not) between the aims of the site administrators and those of the site users. In each case this has resulted in the insertion of community norms into the reputation-assessment system created by and for site use.

In contrast, let us consider for the third example, a situation where the system is designed to facilitate community-derived norms – as an example, the news aggregator site Digg.com.

Though nominally Digg acts merely as a central repository for links that are submitted by users, in fact it operates via sophisticated algorithms that allow users to “digg” or “bury” a particular link. Links that receive many and diverse diggs will be “promoted” to the front page of the site, where links that are “buried” will not appear, a participatory process that Digg.com describes as “[t]hat’s how I get the spam out of the process and let the good stuff rise to the top.”¹⁴¹

The Digg model is based on user contributions – in fact all content on the site is user-submitted. Community members submit links (to news stories, video clips, blog posts, or whatever other content they want to recommend), and those submissions become viewable by other community members, who are able to “Digg” (recommend) or “Bury” the individual items. Content which receives sufficient community Diggs may wind up on the “front page” of the site, viewable by anyone who goes to Digg, not just

¹⁴¹ Digg.com, “How Digg Works” <<http://about.digg.com/how>>.

community members.¹⁴² Items on the front page are marked with the name of (and link to) the original submitter and the time of submission.

Reputation operates in a number of different ways on Digg. In a 2006 interview, Digg co-founder Kevin Rose suggests that there is a behind-the-scenes reputation system in the Digg architecture, but clarifies that it is targeted at spam and fraud detection rather than derivation of user reputation per se.¹⁴³

In the interview, Rose goes on to suggest that if there is a reputational algorithm functioning on the site, it is more focussed on reputation of the story rather than of the submitting user.¹⁴⁴ However, as Richter et al. have noted “[n]evertheless, the influence of an individual user’s votes (so called “diggs”) seems to increase with every successful submission, i.e. one which is subsequently made popular by the community.”¹⁴⁵ This is consistent with the Lerman’s 2006 study that showed that “of the more than 15,000 front page stories submitted by the top 1020 users, the top 3% of the users are responsible for 35% of the stories.”¹⁴⁶

¹⁴² Articles that are destined for the front page generally make it there within the first 2-3 hours, and remain on the front page for about 79 minutes. Fang Wu & Bernardo A Huberman, "Novelty and Collective Attention" (2007) 104:45 PNAS at 17599

¹⁴³ Richard MacManus, "Interview with Digg founder Kevin Rose" (ZDNet, 2006), online: <<http://www.zdnet.com/blog/web2explorer/interview-with-digg-founder-kevin-rose-part-1/108>>

¹⁴⁴ *Ibid.*

¹⁴⁵ Richter, Wolf, Escher, Tobias and Bray, David A., The Performance of Distributed News Aggregators (November 17, 2008). OII DPSN Working Paper No. 9. Available at SSRN: <http://ssrn.com/abstract=1324462> or <http://dx.doi.org/10.2139/ssrn.1324462>

¹⁴⁶ Kristina Lerman, "Social Networks and Social Information Filtering on Digg" (International Conference on Iblogs and Social Media, 2006) [unpublished] 4. Interestingly, Richter et al. discuss the changes made to Digg post-2006 (and thus post-Lerman’s study) but conclude that the distribution of power does not really seem to have changed, despite changes to the system (Richter, Wolf, Escher, Tobias and Bray, David A., The Performance of Distributed News Aggregators (November 17, 2008). OII DPSN Working Paper No. 9. Available at SSRN: <http://ssrn.com/abstract=1324462> or <http://dx.doi.org/10.2139/ssrn.1324462>)

A review of Digg shows that while the site architecture is designed to facilitate community-derived norms becoming the arbiter of content¹⁴⁷, there may be another level of reputation operating here too, this one at the level of social network and friend-circles.

When a user signs up with Digg, they create a profile page which contains basic personal information. The page also displays information about user activity on Digg, including details about submissions, effectiveness in identifying popular stories, and successful submissions. The page also contains a “popular” ratio, which reflects the number of original submissions that make it to the front page.

Community members are able to designate other users as “friends, a relationship that allows them to see what stories their “friend” has submitted, “dugg”, or commented on. Lerman has shown that these friend networks have an influence on content within Digg; that users digg the stories their friends submit as well as the stories their friends have dugg.¹⁴⁸

Richter et al. felt that the power imbalance demonstrated by the heavy influence of power Digg-ers on front page content indicated a “structural imbalance inherent in the normal performance of Digg”¹⁴⁹. While this may be true, I would suggest that some form of imbalance was perhaps inevitable on this model.

¹⁴⁷ Remembering, as established in chapter 1, that popularity – mainstream social acceptance and approval – is an indicia of conformance to normative expectations.

¹⁴⁸ Kristina Lerman, "Social Networks and Social Information Filtering on Digg" (International Conference on Iblogs and Social Media, 2006) [unpublished] 4

¹⁴⁹ Richter, Wolf, Escher, Tobias and Bray, David A., The Performance of Distributed News Aggregators (November 17, 2008). OII DPSN Working Paper No. 9. Available at SSRN: <http://ssrn.com/abstract=1324462> or <http://dx.doi.org/10.2139/ssrn.1324462>

Thus, even in a system whose design was intended to facilitate user-norms defining the content, particular user norms/patterns emerge which come to define the content and reinforce particular norms.

Creation of the Transoptic Norm

In the foregoing discussion of different norms derived and enforced through lateral and synoptic surveillance, I see the intersection of the synoptic and the panoptic that is occasioned through the technology of reputation systems.

Synoptically, community standards are created, normativized, received, and relied upon by community members in their assessments of the 'good' reputation of others – a process of the many watching the many within the context of broader norms derived from synoptic interactions of the many watching the few.¹⁵⁰

The prevailing view is that reputation systems lead to the transformation of decision-making:

...reputations formed from a cooperating network of people have the potential to be better than those any single person could form. Our judgments on any complex topic are inevitably transmitted to each other in an incomplete and distorted fashion. The task of reputation systems designers is then to set up incentives that minimize inaccuracies and maximize productive collaboration so that wherever possible the judgment of a group – or indeed, of an entire society – becomes better than the judgment of its individual members.¹⁵¹

The distinction between synoptic norms and those put in place by the system designers, however, shows how the synoptic standards of the group – or indeed of an entire society – may ground the assessment of reputation no matter how clearly the system is designed to address specific instances or factors. When synoptically derived norms ground or influence the assessment of 'good behaviour' (as they must always

¹⁵⁰ Valerie Steeves personal communication 8 September 2012

¹⁵¹ Hassan Massum & Yi-Cheng Zhang. "Manifesto for the Reputation Society" First Monday 9 (2004)

do) then the reporting/assessing of behaviours that is collected and aggregated in a reputation system is similarly defined. In this sense, system design operates like other instrumental logics by privileging, constraining and pushing against socially derived norms, but never in a way that is determinative of the (meaning of the) interaction because the human interaction that takes place within technical systems is still social.¹⁵²

Reputation systems may, therefore, be designed to address extremely specific behaviours. I've looked at performance in a commercial transaction on eBay and accuracy of self-presentation on an online dating site. The systems are designed and intended to function as a form of surveillance, exerting a regulating force that encourages conformance with the behaviours deemed desirable by the site administrator. It seems, however, that by their reliance on co-veillance and community participation, reputation systems become normative enforcers for standards above and below those they were designed to set and enforce. That is, the synoptically derived norms that users of the site bring with them to the assessment process and that they write in to the reputation system (implicitly if not explicitly) result in the social control exerted by these norms becoming (if unwittingly) transformed into institutional controls and promulgated accordingly. This level of nuance, complexity and individualized decision making stands in sharp contrast to the first requirement for an effective reputation system, which necessitates that the system depend on credible signals.¹⁵³

Nor is it sufficient to speak of system design as a response to this. Given that the norms are derived synoptically, having them encoded in the reputation mechanism will serve the needs of the mainstream users of the site – that is, the judgement of the many will become greater than the judgement of the one site administrator.

¹⁵² Valerie Steeves personal communication 8 September 2012

¹⁵³ *Ibid.*

This is not, then, merely a situation where the synoptic and panoptic are present in the same technology. Instead, what I see in this is a merging that creates a new regulating power – the transoptic, wherein the synoptic is systematized and in so doing achieves institutional and thus regulating force.

Conclusion

Gary Marx has put forward a series of questions that should be asked to ensure the ethicality of any proposed form of surveillance.¹⁵⁴ Reputation systems can and should be put to this rigorous examination.

My point, however, is a larger one. Whether or not reputation systems are an ethical form of surveillance, the fact remains that they are not the neutral technologization of word of mouth that has been venerated as scientific and thus reliable and accordingly joyously celebrated. The derivation, reporting, aggregation and systemic reliance upon reputation has a regulatory effect. It sets the standards of expected behaviour; acts to enforce adherence to those standards by rewarding those who conform to them and stigmatizing those who do not; and they normalize those standards, resulting in the internalization of the standards and the self-policing of behaviour by users. Far from the transformative tool of cooperation that reputation systems purport to be, then, in this environment they have the power to perpetuate (mainstream) inequalities under the guise of supervising to encourage ‘good’ behaviour.

Possibly this has moved beyond the medium as the message, and as such the application of an ethics framework to the medium (surveillance) is no longer sufficient. Carolyn Marvin has suggested that:

...the history of electronic media reveals less about the evolution of technical efficiencies in communication than a series of arenas for negotiating issues crucial to the conduct of social life. Among those issues, who is ‘inside’ and who is

¹⁵⁴ Gary Marx, "An Ethics for the New Surveillance" (1998) 14:3 The Information Society 171 at 44

‘outside’, who may speak and who may not and who possesses authority to be believed. Here, she maintains, the focus of communication is shifted from ‘the instrument’ to ‘the drama’ in which diverse social groups perpetually negotiate power, authority, representation and knowledge with whatever resources they have at their disposal.¹⁵⁵

Building from this framework, therefore, the next chapter will proceed to examine how reputation functions in non-reputation system online spaces in order to explore how reputation shapes participation in those non-reputation-regulated spaces and what norms are being (re)enforced by that shaping.

¹⁵⁵ Sean P. Hier “Probing the Surveillant Assemblage: on the dialectics of surveillance practices as processes of social control” (2003) 1(3) *Surveillance & Society* 399-411.

CHAPTER 3: Non-Systematized Impression and Reputation Management

"In the course of [corresponding with others on the site] I became aware of how I had to present myself" (Male Interviewee)¹⁵⁶

The previous chapter introduced the idea and explored the transoptic force of systematized reputation. That is, how reputation systems designed for one particular purpose may, in the hands of the community, simultaneously become vehicles for the regulation and enforcement of entirely different values and norms from those originally intended. It would be a mistake, however, to presume that this process operates only or solely within online reputation systems. Indeed, as this chapter will argue, this process is neither an artefact of online systems nor of reputation systems themselves. Instead, it is a function of the very processes of identity negotiation and presentation within society(s).

To demonstrate this, chapter 3 will explore identity negotiation and presentation mechanisms in society, and then focus more narrowly on those same processes within the common technosocial environment of the social network site. Doing so will show how, even outside a formal system of surveillance or ranking, a process of identity performance and impression management results in a similarly transoptic force, with its attendant reinforcement of and reward for norm adherence.

Social Network Sites

The field of Computer Mediated Communication is a deep one, and has surveyed many types of online interaction. In discussing online self-presentation, researchers have looked at homepages, blogs, SMS behaviour, email, twitter; indeed, virtually any way that people are able to present a disembodied self in communication has been explored.

¹⁵⁶ Nicole Ellison, Rebecca Heino & Jennifer Gibbs, "Managing Impressions Online: Self-Presentation Processes in the Online Dating Environment" 11:2 Journal of Computer-Mediated Communication (2006) at 9

For the purposes of this project, however, I choose to focus exclusively on identity presentation and regulation in social network sites, since they combine elements of many of the other types of online communication – profile creation, collection of stories and links, communication with others on the site, status updates etc.

The terms “social network site”, “social networking site” and “social media” all appear in the literature, seemingly interchangeably. For present purposes, I choose to use the term “social network site” (SNS). This decision is not merely stylistic – rather, in choosing to emphasize the network as an object rather than the action of networking, I hope to underscore that the primary action of these sites is not (new) relationship initiation but rather the articulation and making visible of social networks¹⁵⁷ both as they exist and as they develop.

A SNS here is defined as:

A web-based site or utility that allows individual users to:

- (a) construct a profile within the site;
- (b) articulate a list of other users with whom they share a relationship or connection; and
- (c) view and traverse their own list of connections as well as lists of connections made by other users of the site.¹⁵⁸

SNSs lend themselves to an examination of reputation in online spaces given that they “already have reputation systems build in... the presumption of trust comes from testimonials and connections to other users.”¹⁵⁹

¹⁵⁷ danah m boyd & N.B. Ellison, "Social network sites: Definition, history, and scholarship" (2007) 13:1 *Journal of Computer-Mediated Communication*

¹⁵⁸ danah m boyd & N.B. Ellison, "Social Network Sites: Definition, History, and Scholarship." *Journal of Computer-Mediated Communication* 13, no. 1 (2007) at 1

¹⁵⁹ Alice Marwick, *Selling Your Self: Online Identity in the Age of a Commodified Internet*, University of Washington, 2005) [unpublished] at 118.

SNSs are also useful for this project because they locate individuals within the context of a larger network or chosen community, just as do the offline processes discussed in chapter 1 and the online reputation systems discussed in chapter 2. SNSs provide a framework for social grooming – a space that facilitates the maintenance of a friendship/community network as well as “the public display of interpersonal commentary.”¹⁶⁰ This may take many forms on an SNS; sharing or re-posting content from others, posting photographs and tagging peers who appear within them, even the way(s) in which users build rapport and strengthen bonds by sharing information and commenting on each other’s content

Profiles and Identity

Users create profiles on an SNS, and these profiles may include photos, lists of personal interest, biographical and contact information. Users are also able to add friends to their profile. Although some SNS (such as LinkedIn) have “premium” paid memberships that convey special privileges, the majority of SNS are, like Facebook, free to users and support themselves by generating revenue from advertisers by means of banner advertising and the like.

When a user first sets up a profile on an SNS, there are nominally two stages – the provision of certain limited information that is required in order to sign-up for an account, and the information that is solicited later by way of prompts to build or fill out a profile. In actuality, an individual setting up a profile goes through the steps as a single process – s/he provides the required registration information, activates the account through email, then proceeds to setting up a profile by providing further information. The SNS generally provides some form of “template” for profile creation, with categories and spaces for users to fill in. Some have suggested that these templates may even be part of the reason for the success of SNSs, because “the questions deemed relevant – who their peers are, what bands they like and so on – have

¹⁶⁰ Judith Donath, "Signal in Social Supernets" (2007) 13:1 Journal of Computer-Mediated Communication at 2

already been decided and are presented to the potential profile maker by the service”¹⁶¹, thus alleviating the user from the responsibility of determining how to best present themselves. In contrast, boyd has argued that notwithstanding the use of such templates “there is plenty of room for [users] to manipulate the profiles to express themselves. At a basic level, the choice of photos and the personalized answers to generic questions allow individuals to signal meaningful cues about themselves.”¹⁶² This duality sets up the same tensions that were identified within formal reputation systems and which led to the development of transoptic force. That is, while templates function to assert norms within the space just as do any insertion of “default” settings in a platform act to assert a legitimating force by setting out normative expectations¹⁶³, there still exists the space for users to insert themselves and their expectations into the interactions on the site as well.

On an SNS there are many identity signals available, the most visible being the profile. Similar to identity in the Mead or Goffman sense,¹⁶⁴ a profile on an SNS is a dynamic entity; “a locus of social interaction that evolves and changes to reflect various dynamics within social networks and communities.”¹⁶⁵ The profile may be thought of as a form of self-presentation, similar to Goffman’s “front stage”, wherein users “engage in impression management by adjusting their profiles, linking to their friends, displaying their likes and dislikes, joining groups, and otherwise adjusting the situated appearance

¹⁶¹ David Brake, “Shaping The “Me” In Myspace: The Framing of Profiles on a Social Network Site.” In *Digital Storytelling, Mediatized Stories: Self-Representations in New Media*, edited by K. Lundy, (2008) at 297.

¹⁶² danah boyd, “Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life” in David Buckingham ed., *Youth, Identity and Digital Media: MacArthur Foundation Series on Digital Learning*, 2007) at 10.

¹⁶³ Nicole Ellison, Rebecca Heino, and Jennifer Gibbs. “Managing Impressions Online: Self-Presentation Processes in the Online Dating Environment.” *Journal of Computer-Mediated Communication* 11, no. 2 (2006) at 16

¹⁶⁴ That is, that identity is constructed by reference to context; we choose how we will present ourselves based on the impression we want to create in all the surrounding circumstances. Accordingly, identity is not something fixed or immutable but rather is an ever-changing performance. Power/authority/structure may produce a seemingly fixed identity, but that identity is still contextual and created.

¹⁶⁵ Zeynep Tufekci, “Grooming, Gossip, Facebook and MySpace: What Can I Learn About These Sites from Those Who Won’t Assimilate?” (2008) 11:4 *Information, Communication & Society* at 546

of their profiles.”¹⁶⁶. This process of situating is an important one; research has suggested that for at least some SNS participants “position in the peer network is more significant than the personal information provided, rendering the profile a place-marker more than a self-portrait.”¹⁶⁷ The profile and the information provided during SNS use, then, are about identity presentation with an end goal of creating and asserting social capital.¹⁶⁸

SNS profiles need to be understood as a form of impression management; as “taste performances” by users who are aware of the impressions they foster. As such, they implicitly include not only the awareness of impressions but some management skill, presentations of identity which are shaped by the context in which they appear and the expectations of the group(s) for whom they are performed.¹⁶⁹ This is not a one-sided performance; these expectations do have an impact, just as they would in offline interactions. This may result in profiles that appear to occlude the “authentic” identity of an individual; profiles that aren’t grounded in any bodily reality; or even profiles which merely appear to represent one aspect of a multi-faceted individual. In each case, users must be understood to be constructing a profile based on their assumptions about the norms of the space they inhabit and the expectations of the audience with whom they interact.

¹⁶⁶ Zeynep Tufekci, “Grooming, Gossip, Facebook and MySpace: What Can I Learn About These Sites from Those Who Won’t Assimilate?” (2008) 11:4 *Information, Communication & Society* at 546.

¹⁶⁷ David Brake, “Shaping the “Me” in MySpace: The Framing of Profiles on a Social Network Site” in K. Lundy ed., *Digital Storytelling, Mediatized Stories: Self-Representations in New Media* (Peter Lang Publishing 2008) at 289., referencing Sonia Livingstone & Magdalena Bober, “UK Children Go Online: Listening to Young People’s Experiences” ESRC (2005), online: <http://www.lse.ac.uk/collections/children-go-online/UKCGO_Final_report.pdf>.

¹⁶⁸ It should be noted as well that both the performance of identity and the exercise of social capital on SNSs are not restricted to SNSs – those with whom a user interacts and from whom they receive signals are as likely to have offline resonance as they do online resonance.

¹⁶⁹ Hugo Liu, “Social Network Profiles as Taste Performances” (2007) 13:1, article 13 *Journal of Computer-Mediated Communication* at 1

Marwick has suggested that SNSs have a form of reputation system built in.¹⁷⁰ Donath expands on this, suggesting that profile information consists of fairly conventional signals which may be easily faked or copied, and that it is the presence of links to other members (the friend network) that purports to authorize these presentations and confirm them as truth. She notes, however, that it is important to be aware that in this scenario “‘true’ means ‘true to the mores of our community’, which can range from strict adherence to known facts to highly imaginative role-playing.”¹⁷¹

These are key recognitions for understanding both how identity construction and performance function within SNS and how that information is context-shaped. From this follows the understanding that its collection and use outside SNS may create false or unreliable signals about trustworthiness and reputation.

Performative Identity

Theories about identity are multiple and stem from a variety of academic disciplines. In this chapter, I shall focus on theories derived from social psychology. Key to this perspective is the understanding that identity is dynamic rather than fixed – that it is a production “which is never complete, always in process, and always constituted within, not outside, representation.”¹⁷²

Hammack grounds the early development of this approach in Cooley’s “looking glass self” and James’ notion of identity as personal self-consciousness, suggesting that they form the base for Mead’s recognition of the interrelationship between self-development and social interaction.¹⁷³ Mead’s recognition was that “selves are constituted by or in

¹⁷⁰ Alice Marwick, “‘I’m a Lot More Interesting than a Friendster Profile’: Identity Presentation, Authenticity and Power in Social Networking Services” *Association of Online Internet Researchers*, (Chicago, 2005).

¹⁷¹ Judith Donath, “Signal in Social Supernets” *Journal of Computer-Mediated Communication* 13, no. 1 (2007) at 5

¹⁷² Stuart Hall, “Cultural Identity and Diaspora” in J. Rutherford (ed.) *Identity: Community, Culture, Difference*, 222-237 (London: Lawrence & Wishart 1990)

¹⁷³ Phillip L. Hammack, “Narrative and the Cultural Psychology of Identity” *Personality and Social Psychology Review* 12 (2008) at 226

terms of the social process and are individual reflections of it.”¹⁷⁴ This conceptualization is an important one, suggesting both an underlying subject/self and a social interaction that influences identity and how it may be constructed.¹⁷⁵ Thus, “identities are performed for others, but also created in the performative social interaction itself.”¹⁷⁶

Within the literature, there are of course arguments about the existence of any essential “self”; whether it is pre-discursive or in fact it is discursively produced.¹⁷⁷ For our purposes, this debate need not be settled since, as Marwick notes, the issue is one analogous to Foucault’s “regime of truth”¹⁷⁸ in that “if a society believes something to be true and acts as if it is true, it does not matter whether it literally is true. What matters is whether people treat it as if it were so. This regime of truth extends similarly to identity performance and symbolic markers.”¹⁷⁹

What this means, at its most basic, is that for the purposes of this analysis, I understand “identity” to be a dynamic process, one that is performed on an ongoing basis and with regard to all contextual factors. This does not necessarily mean that each performance is idiosyncratic and original; rather, what it means is that there are recognized roles in any circumstance, and that these roles are dynamic in regards to the other roles around them. These contextual identities (or roles) are interdependent, meaning that where

¹⁷⁴ George Herbert Mead. "The Realization of the Self in the Social Situation", Section 26 in *Mind Self and Society from the Standpoint of a Social Behaviorist* (Edited by Charles W. Morris). Chicago: University of Chicago (1934): 200-209 at 201

¹⁷⁵ R.G. Dunn, (1997). “Self, Identity and Difference: Mead and the Poststructuralists.” *Sociological Quarterly* 38.4: 687-705. at 693

¹⁷⁶ Phillip L. Hammack, "Narrative and the Cultural Psychology of Identity." *Personality and Social Psychology Review* 12 (2008) at 234

¹⁷⁷ R.G. Dunn, (1997). “Self, Identity and Difference: Mead and the Poststructuralists.” *Sociological Quarterly* 38.4: 687-705. at 693.

¹⁷⁸ Michel Foucault, “Truth and Power.” *Power/Knowledge : Selected Interviews and Other Writings, 1972-1977*. (New York: Pantheon, 1980) 133.

¹⁷⁹ A. Marwick, "Selling Your Self: Online Identity in the Age of a Commodified Internet." Unpublished master's thesis, (University of Washington, Seattle, WA, USA 2005), online: <http://www.tiara.org/papers/amarwick_sellingyourself_mathesis.doc> at 20.

the identity is less certain participants may subtly adjust their role performance in order to explore the roles that others are performing. Individuals, then, attempt always to understand and perform the role that they perceive to be required of them in a given set of circumstances in order to achieve high social integration.

Key to this discussion is the work of Erving Goffman, whose work seems to simultaneously suggest at least the possibility of an essential self, while also recognizing a socially constructed or performed identity. Goffman talked about this in dramaturgical terms, talking about frontstage performative social behaviour while also incorporating a backstage more interior identity.¹⁸⁰

Arguably, there is no full autonomy in either of these categories. Certainly front stage behaviour, like that in a job interview, may involve an individual taking steps to present herself optimally to the audience and thus steer audience perception in a desired direction, but as Vitak notes, these fronts themselves tend to become institutionalized, and conformance to the stereotype becomes necessity rather than a full matter of choice.¹⁸¹ On the backstage, Marwick points out that identity characteristics such as class or gender, while seen as essential, may simply have become so ingrained as to become naturalized.¹⁸²

Understanding how all of this plays out with regard to reputation, then, requires beginning with an understanding of “identity” that views it as reproducing and perhaps even co-creating social norms and conditions even as it is influenced and constructed

¹⁸⁰ Erving Goffman, *Interaction Ritual* (New York: Anchor Books, 1967)

¹⁸¹ Jessica Marie Vitak, *Facebook "Friends": How Online Identities Impact Offline Relationships* (Georgetown University, 2008) [unpublished] at 11.

¹⁸² A. Marwick (2005). "Selling Your Self: Online Identity in the Age of a Commodified Internet." Unpublished master's thesis, University of Washington, Seattle, WA, USA
<http://www.tiara.org/papers/amarwick_sellingyourself_mathesis.doc> at 21.

in reference to those norms. Thus, "through social interaction...the significant symbolic gestures necessary for successful participation in a community are internalized."¹⁸³

The Technosocial is the Social

For Goffman, the two primary factors impacting self-presentation choices were context and audience. That is, people's performances change depending on who they are interacting with and the environment and social structure within which that interaction takes place. Dunbar's understanding of the role of language allows us to understand how context may operate in situations where there is no physical co-presence. As boyd & Heer note, "in lieu of the physical, artifacts of digital performance create the digital body. Through interaction with other digital bodies, the artifacts of performance create the context of a digital environment. People must interpret those performances in order to understand the social context and thus what is socially permissible and expected."¹⁸⁴

It is often tempting, in looking at online interactions, to fall into the trap of believing them to be separate and distinct from offline interactions, and accordingly to attempt to formulate new theories of identity, behaviour and performance in order to understand them. It is my contention that this is, in fact, unnecessary. At their core, social interactions do not change merely because they are expressed through the medium of a computer nor does the underlying identity itself necessarily change.¹⁸⁵ It is, however, fair to say that the process by which that identity is negotiated may change.

¹⁸³ Phillip L. Hammack, "Narrative and the Cultural Psychology of Identity." *Personality and Social Psychology Review* 12 (2008) at 234

¹⁸⁴ danah boyd & Jeffrey Heer, "Profiles as Conversation: Networked Identity Performance on Friendster" (Proceedings of the Hawai'i International Conference on System Sciences (HICSS-39), Persistent Conversation Track, 2006) [unpublished] 4.

¹⁸⁵ See E. Wynn & J. E. Katz, "Hyperbole over Cyberspace: Self-Presentation & Social Boundaries in Internet Home Pages and Discourse." *The Information Society* at 298; A. Marwick, "Selling Your Self: Online Identity in the Age of a Commodified Internet." Unpublished master's thesis, (University of Washington, Seattle, WA, USA 2005), online: <http://www.tiara.org/papers/amarwick_sellingyourself_mathesis.doc> at 109.

Based on his work with primates, Robin Dunbar has suggested that in human sociality, language takes the place of grooming behaviour – that both are inherently social behaviours that serve particular functions.¹⁸⁶ Social grooming often serves the purpose of establishing and enforcing social norms and conventions, as may happen through gossip and other forms of communication. Tufekci notes that it may also be a competitive activity, “a means to improve one’s reputation and status as well as access to resources and social and practical solidarity.”¹⁸⁷ Where language is the medium of this social grooming, it can be said that language “helps people learn about cultural norms, evaluate others’ behaviour, and keep up with the news and shifting opinions of their surrounding community. It makes reputation possible – individuals benefit from the experience of others in determining who is nice, who does good work, and who should be shunned for their dishonest ways.”¹⁸⁸

Language’s role as social grooming is important, for it enables us to move beyond Goffman’s conception of co-presence¹⁸⁹ and towards an understanding of presence that incorporates ideas of telepresence.¹⁹⁰ This is key, because sociality (and thus the presence of others) is central to the development and performance of identity under these theories.

Thus, identities are constructed and roles performed online in response to social cues just as we understand them to be offline. Accordingly, re-viewing the profiles and interactions on SNS can reveal both the social signals and roles being perpetuated within the perceived context as well as providing an opportunity to consider the disconnect between perceived context and actual audience.

¹⁸⁶ Robin Dunbar, *The Trouble With Science*, (Boston: Harvard University Press, 1996) (1996)

¹⁸⁷ Zeynep Tufekci, "Grooming, Gossip, Facebook and Myspace: What Can We Learn About These Sites from Those Who Won't Assimilate?" *Information, Communication & Society* 11, no. 4 (2008) at 546

¹⁸⁸ Judith Donath, "Signal in Social Supernets", *Journal of Computer-Mediated Communication* 13, no. 1 (2007) at 1

¹⁸⁹ Goffman defined co-presence as “experiencing someone else with one’s naked senses”

¹⁹⁰ Jessica Marie Vitak, *Facebook "Friends": How Online Identities Impact Offline Relationships* (Georgetown University, 2008) [unpublished] at 15.

Impression Management

Fiore & Donath have shown that “homophily dominates human attraction.”¹⁹¹ That is, that people are interested in and drawn to those who appear similar to themselves. An understanding of this is essential to understanding the impact of impression management on profile development and presentation, as well as to research in this field.

Many argue that in SNSs, users assess the desirability of potential friends by perusing their profiles.¹⁹² On this surface, this may seem to conflict with research that suggests that SNS users primarily use the sites for the purpose of maintaining ties with those they already know rather than for the purpose of connecting with new people. As discussed earlier, the visibility of friend networks is one of the key indicia of a SNS. It is important to understand that it is not just the existence of this visible network that shapes SNS use, but also the information that is conveyed by such a visible network. Information about an SNS user is not only gleaned from their profile; indeed, the profile may be inherently suspect as it is comprised of signals that are easily falsified.¹⁹³ Earlier I discussed how the existence of friend networks acts as a kind of reputation system, seeming to authenticate the content in a profile. It is not just the existence of the network but the content of it that has this effect; “information about the user’s identity can also be gleaned contextually from the other members of the user’s publicly articulated network.”¹⁹⁴ Thus, the conflict above may be minimized when I understand this finding through the lens of social-psychology and impression management; perhaps rather than assessing “potential friends”, the SNS user is evaluating profiles to

¹⁹¹ Andrew Fiore & Judith Donath, "Online Personals: An Overview" *CHI 21004*, 24-29 (April, 2004)

¹⁹² J. Donath (2007). Signals in social supernets. *Journal of Computer-Mediated Communication*, 13(1), article 12. <<http://jcmc.indiana.edu/vol13/issue1/donath.html>> at 8

¹⁹³ *Ibid.*

¹⁹⁴ A. Marwick, "Selling Your Self: Online Identity in the Age of a Commodified Internet." Unpublished master's thesis, (University of Washington, Seattle, WA, USA 2005), online: <http://www.tiara.org/papers/amarwick_sellingyourself_mathesis.doc> at 104.

assess the desirability of linking to this particular friend or acquaintance in terms of the impact of that link on her own reputation.

This interpretation is buoyed by danah boyd's description of SNS profile authenticity. She writes that youth:

...construct these profiles for their friends and peers to view...while what they present may or may not resemble their offline identity, their primary audience consists of peers that they know primarily offline – people from school, church, work, sports teams, etc. Because of this direct link between offline and online identities, teens are inclined to present the side of themselves that they believe will be well received by these peers.¹⁹⁵

Thus, peer standards insert themselves into profile development and presentation, and impression management is inherently bound up with identifying those standards. It seems, then, that understanding that impressions are formed almost instantaneously, users “attempt to manage these impressions, strategically emphasizing some characteristics while de-emphasizing others.”¹⁹⁶ The characteristics chosen for emphasis or de-emphasis will depend on the context; on the expectations received from the intended audience and the understanding that meeting those expectations garners or enhances social capital.

Brake's research indicated that while all interviewees recognized and were guided by their perceptions of a set of rules/expectations regarding presentation of identity, “the perceived rules were not always the same.”¹⁹⁷ This should not be surprising. Fashions are peer derived, and as discussed, individuals are performing identities shaped by the expectations of their particular group.

¹⁹⁵ danah boyd, "Social Network Sites: Public, Private, or What?" (2007) 13:28 Knowledge Tree

¹⁹⁶ Cliff Lampe, Nicole Ellison & Charles Steinfield, "A Familiar Face(Book): Profile Elements as Signals in an Online Social Network" 2007 [unpublished] 2.

¹⁹⁷ David Brake, "Shaping The "Me" In Myspace: The Framing of Profiles on a Social Network Site." In *Digital Storytelling, Mediatized Stories: Self-Representations in New Media*, edited by K. Lundy, (2008) at . 294.

Fashions and trends may change, but their meaning stays the same, what is important is not what is modelled but rather the timeliness of what is modelled; being up-to-date equates with the acquisition and demonstration of social position. "Fashion is about information, about knowing the changing social meaning of an object or way of doing things."¹⁹⁸ Inevitably there will be fashions and trends in profile presentation, just as there are in other forms of presentation. Given that SNS users have some degree of agency – the ability to manage their self-presentation in the form of information provision¹⁹⁹ – it is unsurprising that they would attempt to strategically present themselves in accordance with current fashions in order to derive increased social position.

Likely all of us remember cliques from our high school years, though not necessarily explicitly articulated or labelled, successful navigation of the high school environment necessitated an understanding of group formation and identities on an almost intuitive level. Similarly, this clustering is visible when one peruses an SNS; "one can see commonalities between groups of friends: some post primarily sex pictures of themselves, while other groups create deliberately abstruse profiles that function as social capital within their peer group or contain specific symbolic markers. Self-presentation strategies are influenced by both the application's structure and the influence of one's social group."²⁰⁰ Participants might not identify themselves as a group or even acknowledge the existence of community boundaries that delineate membership or not, yet the very fact of their presentation, how it is shaped and who it is performed to and for makes those boundaries visible.

¹⁹⁸ Judith Donath, "Signal in Social Supernets" 13:1 *Journal of Computer-Mediated Communication* (2007) at 12

¹⁹⁹ Nicole C Kramer & Stephan Winter, "Impression Management 2.0: The Relationship of Self-Esteem, Self-Efficacy and Self-Presentation Within Social Networking Sites", (2008) 20:3 *Journal of Media Psychology* at 106

²⁰⁰ A. Marwick, "Selling Your Self: Online Identity in the Age of a Commodified Internet." Unpublished master's thesis, (University of Washington, Seattle, WA, USA 2005), online: <http://www.tiara.org/papers/amarwick_sellingyourself_mathesis.doc> at 115.

There is a variety of information available about the way(s) in which individuals present themselves. Kramer & Winter looked at how self-efficacy influenced profile presentation, and found that it correlated with larger friend groups, increased information provision, and informality of style that included riskier and less conservative portrayals.²⁰¹ Some have suggested that this risqué presentation of self is more common in males than in females²⁰² while others see this move towards posting revealing material online as a more general statement, “signalling imperviousness to danger and repercussions.”²⁰³ In contrast, Larsen looked at a Danish SNS and discussed the inclusion of loving/praising paeans from friends within the profile itself as a form of notifying others of their social status and explicitly invoking social context for identity co-construction.²⁰⁴

When discussing identity information within an SNS, it is important not to define the term too narrowly; identity is presented not only in the way in which a user self-represents, but also in the way other users interact with them and what information those contacts present and perform. Indeed, as discussed, self-representation can be seen as somewhat risky since it is most easily falsified. Ellison et al. found that users were aware of this, and in response “sought to show aspects of their personality in their profiles versus just telling others about themselves. They created their profiles with an eye towards stories or content that confirmed specific personality traits rather than

²⁰¹ Nicole C Kramer & Stephan Winter, "Impression Management 2.0: The Relationship of Self-Esteem, Self-Efficacy and Self-Presentation Within Social Networking Sites" (2008) 20:3 Journal of Media Psychology at 114

²⁰² Joy Peluchette & Katherine Karl, "Social Networking Profiles: An Examination of Student Attitudes Regarding Use and Appropriateness of Content" (2008) 11:1 CyberPsychology & Behavior at 96

²⁰³ Judith Donath, "Signal in Social Supernets" 13:1 Journal of Computer-Mediated Communication (2007) at 13

²⁰⁴ Marlene Charlotte Larsen, "Understanding Social Networking: On Young People's Construction and Co-Construction of Identity Online," (Association of Internet Researchers: Let's Play, 2007) at 12

including a laundry list of attributes."²⁰⁵ For others, it is not just the content of the profile but the way one interacts with it. For instance, in Brake's interviews, users expressed the need to change their profile frequently, not in order to reflect themselves, but rather to keep others interested and keep them coming back and remaining linked to the profile.²⁰⁶ Other research showed users reporting highly ritualized behaviours – in one case, the expectation that social events would take place on Thurs/Fri/Sat, photos would be updated on Sunday and thus that everyone would peruse each other's photos on Monday.²⁰⁷ This behaviour is strongly indicative of in-group behaviour, showing not only an expectation of photo uploading on Sunday but also a reinforcement of in-group ties by viewing and commenting on each other's photos regularly. It is in this way that group behaviours – be they expectations about profile content or presentation or about interaction with the SNS and each other – come to reinforce and validate group identities.

Managing impressions in this way has particular importance, not for the profile itself, but for the implications that come from friend linkages. In talking about identity cues, Goffman suggested that we are more likely to privilege cues that are perceived to be unintentional rather than intentional ones. As such, the decision by peers to link to a profile may be held to validate not just the content of the profile itself but the authenticity of the underlying individual.²⁰⁸

²⁰⁵ Nicole Ellison, Rebecca Heino, and Jennifer Gibbs. "Managing Impressions Online: Self-Presentation Processes in the Online Dating Environment." *Journal of Computer-Mediated Communication* 11, no. 2 (2006) at 14

²⁰⁶ David Brake, "Shaping The "Me" In Myspace: The Framing of Profiles on a Social Network Site." In *Digital Storytelling, Mediatized Stories: Self-Representations in New Media*, edited by K. Lundy, (2008) at 290.

²⁰⁷ Bernhard Debatin & et al, "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences"(2009) 15 *Journal of Computer-Mediated Communication* at 96

²⁰⁸ Nicole Ellison, C. Steinfield, & C. Lampe (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication*, 12(4), article 1. <<http://jcmc.indiana.edu/vol12/issue4/ellison.html>> at 2.

Group membership is a strong representation of identity. Boyd notes that “for better or worse, people judge others based on their associations: group identities form around and are reinforced by the collective tastes and attitudes of those who identify with the group.”²⁰⁹ When speaking of groups, I may be talking about peer group behaviour, but some SNSs also allow for users to sign up for interest groups, and those group memberships are also publicly displayed.

Just as publicly displayed friend networks act to reinforce self-representation, so too do group memberships function as an underlying indicia of identity. And these indicia may work both ways; while boyd has discussed the ways that particular group memberships or interest tags may be code for larger affiliations or orientations, MIT Researchers have ascertained that it is possible to identify/predict particular affiliations or orientations (such as homosexuality) based on an analysis of friend networks and group memberships.²¹⁰

Authenticity

Having focussed extensively on the process of impression management and self-presentation aspects of SNS profiles (which are important in an individual’s desire to create, enhance and manage her reputation) it is important to emphasize that this by no means indicates that SNS profiles are inherently false. Returning to the core social psychology analysis discussed at the outset of this chapter, recall that identity is understood as co-created by and with reference to social norms. That is, identity is a social product whereby I perform, you reflect that performance back to me, and I take that reflection into account as I perform in the future. Thus, the “self” is a product of social interaction, a social interaction which also produces, disseminates and reinforces norms. This is not to say that identity is determined by norms, but rather that both

²⁰⁹ danah boyd, "Social Network Sites: Public, Private, or What?" *Knowledge Tree* 13, no. 28 (2007)

²¹⁰ Matthew Moore. Gay men 'can be identified by their Facebook friends'. Mon 21 September 2009, The Daily Telegraph.

identity and norms are social products, dynamically shaped and evolving.²¹¹ Looking at SNSs, Larsen expresses a similar caution about user identity: “the users are very much real and themselves, but at the same time they all expose very reflexive and relational identities. Their identities are continuously constructed through their network and in different situations – they basically exist and become real through their network and those specific situations.”²¹² Thus, the self is neither singular nor determined but continuously and dynamically constructed.

The idea of “authenticity” is, of course, a difficult one, and many have attempted to define it fully. Let us take as a starting point the notion that authenticity is concerned with the conscious self who encounters external forces or pressures or influences that are outside her imagined audience or expected process. In such a case, authenticity may be understood as the extent to which that self is able to remain centered within her identity performance . Applying the idea of authenticity to online representations, Marwick argues that:

...we can identify several different ways in which authenticity operates online. Naturally, users evaluate subcultural performances as authentic or inauthentic in the same way that they would offline, but, due to the lack of visual or bodily cues in internet forums, they use a different set of criteria...forum members claim authenticity through the construction of symbolic boundaries as a means of differentiating themselves as authentic from certain other forum participants whom they see as poseurs. In other words, authenticity online, as defined by users, operates in a similar manner to how it operates offline: by constructing in-

²¹¹ Valerie Steeves personal communication 8 September 2012.

²¹² Marlene Charlotte Larsen, “*Understanding Social Networking: On Young People's Construction and Co-Construction of Identity Online*,” (Association of Internet Researchers: Let's Play, 2007) 15. I would also point out, again, that this reflexive and relational identity construction is not unique to SNSs or to online identities – rather, the individual exists in a context of ongoing sociality and as such individual identity should always be understood as reflexively and relationally constructed.

group/out-group identity and through the display of symbolic markers within self-presentation.²¹³

Of course, just as norms for presentation may vary, so too may ideas of the requisite authenticity. On the SNS studied by Larsen, for instance, authenticity was considered a key value; users were likely not only to publicly identify “fake” profile information but also to source their accusations. Some went even further, creating either separate profiles or entirely separate webpages on which they detailed inauthentic or fake presentations.²¹⁴ Harkening back to the idea of reputation information as surveillance that is effected by reporting on the interactions and performances with a given individual, this makes evident that authenticity is a key value for the particular group studied by Larsen, and that information is accordingly collected and shared as to the degree of authenticity displayed in the identity performance of individuals.

Of course, this is not to say that this focus on authenticity need necessarily be a key factor in all groups. For instance, look to boyd’s work on Fakester profiles within Friendster; profiles that were patently false, purporting to be profiles of fictional characters, objects, or even theories or practices. While the administration of Friendster did not approve of Fakesters and ultimately removed them, for boyd this removal was one of the harbingers of doom for Friendster. Fakesters had become a communication tool and a form of social capital, and their removal signalled a chasm between user interests and the site architecture.²¹⁵

In these two vastly different cases, the desired value or performance varies, but in each case, users who present in the desired manner (building or accruing a positive

²¹³ A. Marwick, "Selling Your Self: Online Identity in the Age of a Commodified Internet." Unpublished master's thesis, (University of Washington, Seattle, WA, USA 2005), online: <http://www.tiara.org/papers/amarwick_sellingyourself_mathesis.doc> at 156.

²¹⁴ Marlene Charlotte Larsen, “*Understanding Social Networking: On Young People's Construction and Co-Construction of Identity Online*,” (Association of Internet Researchers: Let's Play, 2007) at 9

²¹⁵ danah m boyd & N.B. Ellison, "Social Network Sites: Definition, History, and Scholarship." *Journal of Computer-Mediated Communication* 13, no. 1 (2007).

reputation) are likely making conscious decisions about presentation based on context, audience and the in-group understandings of authenticity and performance.²¹⁶ What is key is not what someone outside the group would find authentic or inauthentic, but rather the power of users to “self-regulate the communication and the authority on the website.”²¹⁷

In these spaces, then, authenticity is not only user-regulated, but is linked to information and more specifically to in-group norms. Again, this is not restricted to online spaces. Thornton’s study of UK club culture showed a similar pattern where tastes were governed by “subcultural capital; access to and knowledge of underground and cult markers of cool.”²¹⁸ There is simply an increased focus on information in online spaces due to the lack of other markers by which to judge. Thus, “information fashions” are used to “create virtual walls, allowing those in the know to recognize others within their subculture via their common understanding”²¹⁹ and to identify those who are inauthentically claiming membership to be identified.

Conclusion

In the development and performance of these SNS profiles, then, I see a duality for the users – a need for the individual to present herself authentically while at the same time presenting an identity in accordance with the norms of the space in which she finds herself.²²⁰ This may be further complicated by the normalizing of these performances;

²¹⁶ A. Marwick, "Selling Your Self: Online Identity in the Age of a Commodified Internet." Unpublished master's thesis, (University of Washington, Seattle, WA, USA 2005), online: <http://www.tiara.org/papers/amarwick_sellingyourself_mthesis.doc> at 111.

²¹⁷ Marlene Charlotte Larsen, “*Understanding Social Networking: On Young People's Construction and Co-Construction of Identity Online*,” (Association of Internet Researchers: Let's Play, 2007) at 9.

²¹⁸ Hugo Liu, "Social Network Profiles as Taste Performances." *Journal of Computer-Mediated Communication* 13, no. 1 (2007) at 5 citing Thornton, 1996.

²¹⁹ Judith Donath, "Signal in Social Supernets" 13:1 *Journal of Computer-Mediated Communication* (2007) at 9.

²²⁰ Jessica Marie Vitak, *Facebook "Friends": How Online Identities Impact Offline Relationships*, Georgetown University, 2008) [unpublished] at 10.

a move by the individual to act in accordance with the performance, whether because of internalization or simply because of an innate desire for coherence.

In the previous chapter, I examined reputation systems and demonstrated how they incorporated dual levels of norm policing in order ultimately to perpetuate (mainstream) inequality under the guise of supervising good behaviour. Within an SNS there is no such formal reputation system. This does not mean, however, that there is no need for “good” behaviour.

In looking at reputation systems, I identified two levels of policing: (1) an instrumental notion of good evinced by the site administrator desire to instantiate good behaviour, as dictated by the requirements of the site; and (2) a social notion of good as conforming to expectations as in the norms of the larger community, which were synoptically derived and inserted into the larger system.

At the site administrator level, it is arguable that there is less need to instantiate specific good behaviours. Indeed, the main focus within an SNS is information, and to that end openness is a “designed aspect of the system...to fulfill one’s goal often requires a more permissive approach to profile privacy.”²²¹ This openness is, however, key to the effective functioning of the SNS both on the meta-level and on the individual user level.

The norms of the community arguably take on a larger role in SNSs. Chapter 2 examined formal reputation systems which were designed with particular goals and norms in mind and showed how the norms of the community infiltrated that existing system. An SNS is not the same as these formally designed systems²²² and the norms of

²²¹ Adam N. Joinson (2008). Looking at, looking up or keeping up with people? Motives and use of Facebook. (*SIGCHI* 2008) 1027 at 1036.

²²² Although it is fair to say that they are structured by instrumental norms designed into the system to encourage and privilege certain kinds of performances for the a-social ends of the site through commodification of those performances, the difference is that the formal reputation systems built in

the user community more explicitly shape the performances within the SNS. Where previously they infiltrated an existing system, within SNSs they are (at least to some extent) the system. That is, if a key feature of SNSs is the visible display of a friend network, then such connections become an inherent and integral feature of SNSs. Both the fact of this display of connections and the visibility of the profile come to form a kind of reputation system, where as discussed, the linking of individuals to one's profile as friends implicitly signals not simply a connection but an authentication or validation of that profile.

As discussed, the validation of the profile content does not automatically indicate that what is represented in a profile is accurate; rather, it seems to measure whether in-group norms and expectations are being met in the profile self-representation. Accordingly, the reputation function of the friend network acts to reinforce norms through participation in the SNS, just as norms are reinforced via participation within a formal reputation system.

As for whether these norms are internalized or merely performed for peer recognition, both the user-regulated focus on authenticity and the social psychology conceptions of the interrelationship between identity and self-representation certainly suggest a degree of internalization. This is bolstered by research which indicates links between the design of social systems, the expectations of system participants, and the modelling of behaviour.²²³ Thus, even outside a formal system of surveillance, a process of identity performance and impression management results in a similar reinforcement of and reward for norm adherence, which in turn results in the reputation with which an

norms to regulate user behaviour, where in SNS the norms are built in not to regulate behaviour so much as to facilitate the business case of the SNS with regard to commodification of user information.

²²³ See Andrew Fiore & Judith Donath, "Online Personals: An Overview." *CHI 2004*, 24-29 (April, 2004) ; Nicole Ellison, Rebecca Heino & Jennifer Gibbs, "Managing Impressions Online: Self-Presentation Processes in the Online Dating Environment" 11:2 *Journal of Computer-Mediated Communication* (2006) at 3

individual is tagged being much more a report of norm adherence than of actual performance and reliability.

CHAPTER 4: Out of Context: External Uses of Reputation Information

This is the final chapter in Part I of this dissertation, which sets out to develop a deeper and fuller understanding of the issue of reputation.

The previous three chapters in Part I have established a number of propositions.

Chapter 1 established that reputation is a social artifact – the product of social norm conformance and risk analysis, which themselves are integrally related to the trust assessment that informs individual decisions about whether or not to make oneself vulnerable by assuming risk.

Then chapter 2 showed how formal reputation systems function as a form of surveillance, acting both as the product of and reinforcement for particular normative expectations of behaviour (by design and via the imposition of an overlay of participant expectations), creating and exerting a transoptic force.

Finally, in chapter 3 these ideas were expanded to show that just as an intersection of norms, expectations and risk analysis takes place within formal reputation systems. A similar process operates at a personal and social level in non-formalized reputation situations. That is, even outside of a formal system of surveillance, a process of identity performance and impression management results in a similar reinforcement of and reward for norm adherence.

Taken together, these chapters illustrate the multi-faceted and complex nature of the concepts of “identity”, “reputation” and “trust”. In the remaining chapters, I will use the term “reputation” as an overarching term; when discussing “reputation” I am speaking of the information provided by an individual and by others, the identity performances in which that information is implicated; the inferences drawn by others from available

information; and the overall assessment that may be derived from the analysis of such information and inferences.

I start then with an understanding that the ways that identity is performed and experienced in online spaces are nuanced and subtle, containing within them multiple resonances including racialized, gendered and classist implications. Building from that, I will move now to explore the contexts in which these processes take place in order to generate a holistic understanding of the full context of these transactions and why that context matters

Having situated the behaviours, I start by exploring the ways in which that information operates for and against its subjects. First, I do this by showing how third parties form impressions, and collect and use information within particular spaces intended for a particular audience. Next, I examine how that same information is repurposed. Finally, I discuss how the use of that information and the reputation(s) derived from it become implicated in a *de facto* gatekeeper process, being employed to facilitate the sharing or refusal of information, community participation and access to services.

Mediated Publics

It does not require spending too much time on the Internet to discover the widely shared belief that online information is “inherently public.” But is this always the case?

Fundamentally, the question is whether SNS is in fact a public space. Those to whom this seems obvious suggest that any attempt to conceptualize SNS as non-public is simply the result of confusion about “what is private and what is public on the Internet.”²²⁴ Writing this off as mere confusion, however, simply encourages an increase in education around Internet use generally and SNS specifically; an approach

²²⁴Electronic Privacy Information Center “Social Network Sites and Virtual Communities” in *Privacy and Human Rights Report 2006* (Washington DC, EPIC, 2007), online: <<http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Social.html>>.

which does not seem to have been entirely effective thus far. Instead, a proactive approach to analyzing the said public nature of SNS must begin with an inquiry into the presumptive binary opposition of public and private.²²⁵

Avoiding the binary, danah boyd posits SNS as a “mediated public” – that is, an environment “where people can gather publicly through mediating technology.” She suggests that mediated publics differ from physically public spaces in having four unique features: (1) permanence of record; (2) searchability; (3) replicability/portability; and (4) invisible audience.²²⁶ It is my contention that just as an SNS may be conceptualized as a mediated public, so too might online spaces and communities more generally be re-viewed within this framework.

The idea of mediated publics leaves the public/private divide undisturbed, preferring instead to attempt to nuance the public-ness of the information at issue and by so doing to distance it from traditional treatment(s) of public information.

Helen Nissenbaum, in contrast, has challenged the dichotomy itself. Looking at the dichotomy, she sets out three ways in which the dichotomy acts as a framework for privacy (claims against public/government actors; claims of invasion into private spaces, and challenges to the collection and disclosure of private information) and suggests that, traditionally, anything outside these three areas has been considered

²²⁵ The public/private divide is an area much theorized and discussed, Predominantly, it is held to refer to the distinction between the world of State institutions and protection, paid employment, civic participation (public) and the domestic world that takes place outside the gaze of the State, being instead within the household or family. For discussion of this distinction, see for example: Susan Boyd, “Introduction” *The Public/Private Divide: Feminism, Law, and Public Policy* 12, Susan Boyd, ed. (1997); Ruth Gavison, “Feminism and the Public/Private Distinction”, 45 *Stan. L.R.* 1 (1992); Frances Olsen, “Feminist Critiques of the Public/Private Distinction”, 10 *Constitutional Commentary* 319-27 (1993); Carole Pateman, “Feminist Critiques of the Public/Private Dichotomy” *Public and Private in Social Life* 281, S.I. Benn and G.F. Gaus eds. (1983); Jeff Weintraub, “The Theory and Politics of the Public/Private Distinction” *Public and Private in Thought and Practice: Perspectives on a Grand Dichotomy* 1, Jeff Weintraub & Krishan Kumar, eds. (1997) among others.

²²⁶ danah boyd, “Social Network Sites: Public, Private, or What?” *Knowledge Tree* 13:28 (2007).

inherently public and thus fair game. She critiques this, noting that “the trouble with this approach is that it neglects a range of situations – from those involving nongovernmental actors, to spheres not typically deemed to be personal or private – in which many people perceive robust and legitimate privacy claims.”²²⁷

It is important to note that Nissenbaum herself qualifies that she is not seeking to dismantle the public/private dichotomy but rather she wants to show that it is not:

...useful as the foundation of a normative theory of privacy. Although in the past, it might have served as a useful approximation for delineating the scope of a right to privacy, its limitations have come to light as digital information technologies radically alter the terms under which others – individuals and private organizations as well as government – have access to us and to information about us in what are traditionally understood as private and public domains.²²⁸

My project is not specific to privacy nor the development of a privacy framework as was Nissenbaum’s. That said, both Nissenbaum’s disruption of the traditional public/private divide and her insight into the ways in which digital technologies are blurring the line between public and private are relevant to my discussion of identity and reputation.

Audience and Context

Physical environments provide clues as to what is appropriate; both to those within them and to those who seek to interpret those interactions. Participants in an online space may similarly be able to interpret and act on social cues that are present in those spaces. However, a major issue in this arena comes from those who take information from an SNS and use it while failing to understand (or to even trying to understand) the context in which that information was created and intended. Thus, we have a variety of outsiders drawing inferences from online information and the fact that it was put

²²⁷ Helen Nissenbaum, “Privacy in Context” (Stanford: Stanford University Press, 2010) at 114.

²²⁸ Helen Nissenbaum, “Privacy in Context” (Stanford: Stanford University Press, 2010) at 116.

online in the first place, while simultaneously we have Facebook expert Jesse Hirsch testifying that expressions on Facebook are over-dramatized and not intended to be taken seriously.²²⁹ There is a disconnect here, and it is located in a failure to understand the context in which these interactions take place and how that context informs the actors and actions themselves. This is not to say that the difference is one of physical space vs. online space; rather, I believe that the difference is the result of the rules and expectations of spaces being socially negotiated by their participants. Thus, when outsiders go into a space they don't understand and remove information, they are unable to correctly interpret and understand the cues that may be contained within the information and the context.

Previous chapters explored the ways that people seek to define social situations by using contextual cues. This is intuitively understood in offline environments; in analyzing offline utterances or performances it is easy to identify who is the speaker and who the recipient, therefore allowing an understanding of the social interaction between them and thus to an understanding of context.²³⁰ Social norms emerge situationally, as people learn to read cues and the people present begin to understand what appropriate behavior is.²³¹ However, just as online spaces remove cues from the

²²⁹ Shannon Kari "Facebook Comes to a Head" *National Post* (2008).

²³⁰ danah boyd & Jeffrey Heer, "Profiles as Conversation: Networked Identity Performance on Friendster" in *Proceedings of the Hawai'i International Conference on System Sciences (HICSS-39) Persistent Conversation Track*, Kauai. HI: IEEE. Computer Society. January 4-7 2006 at 4

²³¹ When speaking of spaces and cues, it is tempting to reduce the analysis to physical cues and thus to address this disconnect by pointing to an absence of physical bodies and thus of their cues in online spaces. This argument, in fact, is a product of the very lack of understanding I seek to identify here. Indeed, as Lisa Nakamura and others have pointed out, the presumption that an online identity is disembodied is itself false – gender, race, class and other “embodied” characteristics are written into the identities we create and perform. See for examples: Jenny Sunden, “What Happened to Difference in Cyberspace? The (Re)Turn of the She-Cyborg” (2001) *Feminist Media Studies*, 1:2 215-232; Margaret Chon, “Erasing Race? A Critical Race Feminist View of Internet Identity-Shifting” (1999-2000) *J. Gender, Race & Justice* 439-473; Judith S. Donath, “Identity and Deception in the Virtual Community” *Communities in Cyberspace*, P. Kellock & M. Smith, eds. (London: Routledge, 1999); Radhika Gajjala and Annapurna Mamidipudi, “Gendering Processes Within Technological Environments: A Cyberfeminist Issue” (Spring 2002 *Rhizomes* (4), online: <<http://www.rhizomes.net/issue4/gajjala.htm>> ; Lori Kendall, *Hanging Out in The Virtual Pub: Masculinities and Relationships Online* (Berkeley: University of CA Press, 2002); Lisa Nakamura,

process of social interpretation, so too do they remove the easy identification of audience and context.

In online spaces, the invisibility of audiences makes it difficult for individuals to shape their interactions for the actual audience. Not only can one not “see” one’s audience, but the persistence, searchability and replicability factors of mediated publics mean that audiences who were not present nor conceived of at the time of utterance may nevertheless form part of the audience. boyd suggests that this is, in fact, one of the niches that friends lists fulfill; that given the impossibility of speaking to everyone across time and space, individuals on SNSs instead use friends lists to “imagine who you are speaking to and direct your energies towards them, even if your actual audience is quite different.”²³² Others agree, suggesting that SNS users communicate to a “micro-audience of a subset of their friends”, and that removing utterances from that context changes the imagined expectations of the utterer²³³. Put in public/private dichotomy terms, the friends list purports to reject the presumptive publicness of the utterance, setting out instead a private sphere to whom the information is being communicated and with whom it is intended to be shared

This idea of the imagined audience stems from SNS analysis, and maps extremely well onto the public display of contacts that is integral to an SNS, however it also operates within other sites including those who use formal reputation systems. A site using formal reputation has a different notion of the purpose of the imagined audience. On the one hand, individuals using the site will understand themselves to be

Digitizing Race: visual cultures of the Internet (Electronic Mediations, University of Minnesota Press 2007); Jodi O'Brien, "Writing in the Body: Gender (RE)Production in Online Interaction" Communities in Cyberspace, O. Kellock & M.A. Smith, eds. (Longdon: Routledge, 1999); Rhonda Shaw, "Our Bodies, Our Selves, Technology and Questions of Ethics: Cyberfeminism and the Lived Body" Australian Feminist Studies 18:40 (2003) 45-55; Ken Yoshino, Covering: the hidden assault on our civil rights (Random House 2006)

²³² danah boyd, "Social Network Sites: Public, Private, or What?" *Knowledge Tree* 13:28 (2007).95. It should be noted, however, that while a friends list may account for the imagined audience, it does not account for those who watch (public or private agencies) and are never part of the intended audience.

²³³ Fred Stutzman, "How Facebook Broke Its Culture" *Unit Structures* (2006).

communicating with everyone on the site (rather than a focussed subset of friends). On the other hand, the interactions are site-specific, which means that unlike the virtually limitless audience on an SNS, this imagined audience will be smaller, focussed only on whatever aspect of commerce or connection the site itself is dedicated to. I have already shown how the norms and expectations of such a community are internalized and re-presented to that community, essentially creating a similar impact of imagined audience to that which we see when SNS profiles are shaped by peer group expectations and norms.

Moving from categories towards a new way of understanding and articulating privacy interests, Nissenbaum speaks of the importance of norms and information flows. Collapsing roles, activities, norms, and values into an overarching category of “contextual values”, she proceeds to articulate her understanding of context.

Contexts are not formally defined constructs, but, as mentioned earlier, are intended as abstract representations of social structures experienced in daily life....Because contexts are essentially rooted in specific times and places, their concrete character in a given society, reflected in roles, practices, norms and values, is likely to be shaped uniquely by that society in relation to the arrangement of other contexts in that society as well as to its culture, history, politics and economic, and even to physical and natural contingencies.²³⁴

Thus, the contextual values operant in any particular situation are heavily dependent on multiple factors and can only be understood against the backdrop of the particular interactions and (inter)actors shaping them. Recall in chapter 1 the discussion of H.L.A. Hart’s distinction between internal and external perspectives of law. A viewer who lacks knowledge of the laws which inform the behaviour must inevitably see the behaviour as random or arbitrary. However, when viewed in context against the backdrop of laws, the behaviour becomes comprehensible in a new way. I would suggest that context operates similarly – that context transforms behaviours from

²³⁴ Helen Nissenbaum “Privacy in Context” Stanford: Stanford University Press, 2010) at 134

seemingly random or arbitrary happenings into representations of normative contextual values.

A useful example of how understanding context can transform the understanding of behaviour can be found in Daniel Solove's discussion about the "dog poop girl"; an incident where photos of an individual transgression (a girl allowing her dog to poop on the train and not cleaning it) were taken on a metro train and posted to the internet. Solove argues that "[u]nder existing notions, privacy is often thought of in a binary way – something is either private or public. According to the general rule, if something occurs in a public place, it is not private. But a more nuanced understanding of privacy focuses on transformation via transplant, the way that this case took an event that occurred in one context and significantly altered its nature by making it permanent and widespread."²³⁵ The nature of the event is not changed merely via wide dissemination but rather it is changed by removing it from the context in which it occurred. Context mediates not only an actor's reading of appropriateness but also a reader's understanding of the full implications of the act. When information is removed from the context of SNS and presented as undisputed "fact", readers are prevented from fully understanding the nuances of meaning and weight that should properly be accorded to it.²³⁶

Another example of this can be found by looking at the events that led to the creation of the Holla Back project²³⁷ in New York City. On the afternoon of 19 August 2005, Thao Nguyen was taking the New York City subway back to her office when a man sat down

²³⁵ Daniel J. Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (New Haven: Yale University Press, 2007) at 7

²³⁶ Various takes on this principle may be seen in the comments attached to Alec Saunders, "A Privacy Manifesto for the Web 2.0 Era" *GigaOM Blog* (2008). and specifically in the different characterizations of the Coble/Facebook/Place incident. While some argue that once people had fronded Scoble they implicitly gave him permission to do what he would with their data, others argue that this permission was given only within the Facebook space, and that taking the information out of that space transcended the limited permissions of friending.

²³⁷ <http://www.ihollaback.org/>

across from her, extracted his penis from his pants and began to masturbate. Nervous and wanting to feel safer, she removed her camera-enabled cellphone and eventually took a picture of the masturbator. He left the train at the next stop. Ms. Nguyen immediately reported the incident to a police officer. She went further than that, however – she also posted the photo and an account of the incident on Flickr and Craigslist.²³⁸ This resulted in the cellphone picture being reproduced in the New York Daily Mail the next day, which led over 2 dozen people to identify the offender who was arrested and charged with public lewdness. He pled guilty and was sentenced to two years' probation, with mandatory counselling. Since I first learned the story, I've been fascinated by the comments made by Dan Hoyt (the masturbator in the story) in a New York magazine piece:

In his account, the perpetrator is Nguyen, who misread his intentions (he claims he was already mid-masturbation when she stepped onto the train) and then humiliated him by posting his picture on the Web. He says he didn't even realize he'd been photographed. "Even so, I wouldn't imagine somebody throwing it up on the Internet for millions of people and destroying your life like that," he says. "It's one thing to take it to the police. But on the Internet, I read a lot of people saying, 'That was not too cool of her. That was really screwed up.' "

Hoyt believes that if he and Nguyen had only met under different circumstances, she might really like him. "You know, she'd go, 'That guy's pretty cool. He's got this restaurant, and he's fun,' " Hoyt says. "She'd probably want to go out with me." ²³⁹

Looking at Hoyt's comments, it seems clear that Solove's point about appropriateness being context-dependent has multiple resonances here. Even leaving aside Hoyt's bizarre suggestion both that despite its public setting his behaviour was somehow

²³⁸ This shows how taking things out of context may be an act of power. Sometimes, as here, a taking back of power and using it to enforce accountability; other times, as when mainstream agencies appropriate information from marginalized spaces, as a reinforcement of existing power.

²³⁹ Russell Scott Smith, "Onan the Vegetarian: The Story of a Raw Food Guru Turned Subway Pervert" *New York Magazine* (2006)

private (or at least none of Nguyen's business since it wasn't intended for her), his reading of himself as a victim in this situation due to what he sees as Nguyen's inappropriate behaviour in taking the photograph in the first place and then in making it public shows Solove's point in action – that it “wasn't cool” of her to take his picture in one context (that he considered to be private) and then to make the picture visible in another context (public), thus destroying his life.

Peluchette & Karl looked at questions of access to information contained on SNSs in their research. They found that that respondents were quite comfortable with friends, classmates or family having access to their SNS profiles, but most were ambivalent about employer or stranger access. In fact, 20% of respondents explicitly indicated that their SNS profiles contained information that “they would not want current or prospective employers to see.”²⁴⁰ Generally, this behaviour took the form of references to alcohol or illegal drugs, substance-related photos or comments, and comments from friends that might be deemed inappropriate outside the peer circle. Chapter 3 explored at least some of the forces that shape the decision to put information online (as well as what information is put online) – this, in combination with the idea of an imagined audience who has access to them helps to define the context in which these utterances are made. That context is beautifully characterized by Ibrahmin, who suggests that online networks be thought of as “complicit risk communities where personal information becomes social capital which is traded and exchanged.”²⁴¹ It is key to understand that these utterances, these performances, these risks are undertaken within a particular community and are done with a view to acquiring social capital

²⁴⁰ Joy Peluchette & Katherine Karl, "Social Networking Profiles: An Examination of Student Attitudes Regarding Use and Appropriateness of Content" *CyberPsychology & Behavior* 11:1 (2008) <<http://www.uwlax.edu/faculty/brooks/bus230/handouts/facebook%20article.pdf>> at 33. Students were asked to rate their responses on a scale of 1-5, with 5 indicating strong agreement and 1 indicating strong disagreement. The responses read as “neutral” when it came to access by employers or strangers.

²⁴¹ Bernhard Debatin & al, "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences." *Journal of Computer-Mediated Communication* 15 (2009) at 87

within a particular community, and that the risk that the information may travel outside that context is assumed by all the members of that community.²⁴²

As discussed previously, these online identity performances are self-reflexive and by focussing on the imagined audience, users are explicitly identifying a context to shape their performances. Observers often believe that any or all information posted online is inherently public, and this presumption gets bolstered by the argument that many of these sites, again especially SNSs, have privacy tools that users are not actually applying.²⁴³ Research indicates, however, that the absence of (or failure to adhere to) current mainstream privacy standards does not indicate an absence of privacy or the desire for privacy altogether. From historical early America²⁴⁴ through to contemporary youth online engagement²⁴⁵ we see recognized community norms that facilitate the recognition and protection of privacy even where no physical or spatial privacy is possible.

Various information control strategies are attempted by users. Some users provide false or incomplete profile information or even create multiple online identities and profiles in an attempt to “manage” their privacy. Others have begun to challenge SNS surveillance by undermining it; students at the George Washington University famously

²⁴² As has already been mentioned, it must be recalled that the SNS space is one designed to elicit information for the purposes of commodifying and capitalizing upon it, a purpose that is at the very least at odds with the uses to which users put it and undertake risk to facilitate it.

²⁴³ This is not to suggest that SNS information to which privacy filters have been applied is excluded from this presumptive publicness. Indeed, in *Frangione v Vandongen et al* (2010) ONSC 2823 the court discusses this question, stating at para 38 that: “[The plaintiff] permits some 200 “friends” to view what he now asserts is private. This is a preposterous assertion especially given his testimony that only five of the 200 are close friends. In my view, there would be little or no invasion of the plaintiff’s privacy if the plaintiff were ordered to produce all portions of his Facebook site.”

²⁴⁴ David Flaherty, *Privacy in Colonial New England* (University of Virginia Press, 1972)

²⁴⁵ Valerie Steeves, "Young Canadians in a Wired World, Phase II - Trends and Recommendations" (Ottawa: Media Awareness Network, 2004), online: <[<http://www.media-awareness.ca/english/research/YCWW/phaseII/;>](http://www.media-awareness.ca/english/research/YCWW/phaseII/); For discussion of privacy strategies outside online spaces see also Robert F. Carey "Mobile Telephony in Quiet Places: Territoriality and the Regulation of Noise" (2006).

advertised a massive “beer blast” on Facebook, and when the campus police arrived to bust the partygoers all they found was a sedate event with 40 students and tables of cake and cookies decorated with the word “beer”.²⁴⁶ It is, therefore, a mistake to either presume that the seeming publicness of the space vitiates privacy interests or to assume that no privacy practices are being initiated by users of SNS.

Writing specifically about youth responses to privacy invasions, boyd notes that:

Teenagers are facing these complications head-on and their approaches vary. Some try to resumé-ify their profiles, putting on a public face intended for those who hold power over them. While this is typically the adult-approved approach, this is unrealistic for most teens who prioritize socialisation over adult acceptance. Some teens work to hide their profiles by providing false names, age and location. This too is encouraged by adults, typically without any reflection on what it means to suggest lying to solve social woes. Yet because of the network structure, it's not that hard for motivated searchers to find an individual through their friends.

Another common approach is to demand adults understand these sites as *my* space. In other words, why expect teens to act like they're in school when they're not?²⁴⁷

Again, I want to suggest that these behaviours are not unique, either to SNS or to youth. Indeed, one of the fundamental underpinnings of the “if it's on the Internet its public” attitude is the recognition that it's never that hard for motivated searchers to find information no matter what precautions or obfuscations are employed. Questions

²⁴⁶N. Haas, "In Your Facebook.com" *New York Times* (8 January 2006) at

http://www.nytimes.com/2006/01/08/education/edlife/facebook.html?pagewanted=all&_r=0

²⁴⁷danah boyd, "Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life." In *Youth, Identity and Digital Media*, edited by David Buckingham, MacArthur Foundation Series on Digital Learning (2007) at 131. Recent media reports that youth are leaving SNS in favour of twitter in order to avoid parental surveillance would appear to show that this strategy remains current. See, for example, Barking Robot, "Trend Watch: Teens Leaving Facebook for Twitter: Here's Why" (29 January 2012) at <http://www.debaird.net/blendededunet/2012/01/teens-leaving-facebook-for-twitter-heres-why.html>.

about the accuracy, reliability or even truthfulness of the information that can be found in this way are left unaddressed by this presumption

External Uses of Online Information

The accessibility of this information, combined with its lack of reliability or relevance, is another part of the reason why reputation concerns must be examined and addressed. Where reputation information – formally or informally derived – is being used by third parties for risk and trust analysis there is a risk that the information will be accorded more weight than is deserved. As Cohen points out, “the impetus for the destruction of privacy is a perceived equivalence between information processing and truth. We value information, including personal information, because we believe it will bring us omniscience, and with it the ability to predict preferences, behaviours, and needs and the opportunity to shape public (or private) policies accordingly.”²⁴⁸

Accordingly, as online engagement increases, so too does the collection of information from those spaces by external bodies, be they employers (current or prospective); educational institutions; lawyers; law enforcement bodies or even the State itself.

EMPLOYMENT

Digital “footprints” on the internet may have an impact both pre-employment and post-employment, and these impacts may disproportionately affect non-mainstream groups whose reputations are being assessed against standards not their own.

On the principle of collecting the most information possible upon which to base a decision, it is well-recognized that employers are conducting online “background checks” in addition to criminal record checks and credit bureau checks (where

²⁴⁸ Julie E. Cohen "Privacy, Ideology and Technology: A Response to Jeffrey Rosen." *Geo.L.J.* 89 (2000-2001) at 2031

permitted).²⁴⁹ Indeed, a 2007 survey of 250 US employers found that 44% of employers used SNS to examine the profiles of job candidates.²⁵⁰ 2006 Survey data from ExecuNet demonstrates a similar pattern, with 77% of executive recruiters using web search engines to research candidates and 35% of those stating that they had ruled candidates out based on the results of those searches.²⁵¹

The extent to which this practice is legal remains to be seen – various interpretations have been applied in international jurisdictions. In the United States in May 2007, the U.S. Court of Appeals for the Federal Circuit recently ruled that using Google to investigate an employee did not violate that employee’s right to fundamental fairness.²⁵² In contrast a bill was recently introduced in the Illinois General Assembly that would prevent prospective employers from accessing social network information about prospective employees, including barring requests for usernames or social network passwords from applicants for the purposes of background checks.²⁵³ Internationally, Finland has enacted strong legal prohibitions against employers performing online investigations of employees or prospective employees. Where an employer collects information from a source other than the employee or applicant themselves, consent for the collection must be obtained.²⁵⁴

²⁴⁹ See for example Amy Hockert, “Employers Use “Facebook” and “MySpace” to Weed Out Applicants,” September 9, 2006 <<http://www.wtlv.com/tech/news/news-article.aspx?storyid=64453>>. As revealed in a 2008 special issue of Privacy Scan on the issue, even some of those working within the privacy field use such searches as a pre-employment tool. Murray Long. 2008.

²⁵⁰ Financial Week. Facebook a Risky Tool for Background Checks, Lawyers Warn. (11 March, 2008), online:<<http://www.financialweek.com/apps/pbcs.dll/article?AID=/20080311/REG/234697944>>.

²⁵¹ ExecuNet.com. Growing Number of Job Searches Distrupted By Digital Dirt. Press Release (12 June 2006), online: <http://www.execunet.com/m_releases_content.cfm?id=3348>.

²⁵² As discussed in Declan McCullagh. Police Blotter: Fired Federal Worker Sues Over Googling. (9 May 2007) at http://news.cnet.com/2100-1030_3-6182333.html. It should be noted, however, that the court found that the results produced with the search that the complainant was concerned with did not factor into the decision to dismiss the employee and thus no violation of fairness had occurred. It is difficult to say whether the decision might have been different had the information been relevant and applied in the decision or if the search had been pre-employment rather than as part of a disciplinary proceeding.

²⁵³ US, HB 3782, *Right to Privacy - Social Net*, Re. Sess, Ill 97th Gen Assem, 2011-12

²⁵⁴ Linksandlaw.com. Links&Law: Don't Google Job Applicants in Finland. (4 May 2007) at <http://www.linksandlaw.com/news-update49-job-applicants-finland.htm>.

In countries such as Canada where no similar legal protection has been enacted²⁵⁵, liability comes into play not in the act of searching but on the question of whether hiring decisions are being made based on inappropriate information. At risk is not just actual information found in such a search, but also in the (unfair and possibly gendered, classed or sexualized) inferences that may be drawn from information contained on the site.

As mentioned, recently there has been much discussion about SNS passwords and employment, leading to a number of State and provincial laws introduced to prevent employers from requesting SNS passwords from job applicants.²⁵⁶ While well-intentioned, such legislative initiatives do not truly address the issue. That is, these proposals are targeted at protecting the password to an SNS site, but the real issue is not the password but the information to which that password provides access. As noted above, this information may be available (depending on the privacy settings employed by an individual user) without the password, by means of searching. Thus, if the intent is to protect the personal information of an individual from being accessed and used by a prospective employer, then the legislation must go beyond protecting a password and instead address the real issue. To date none of the proposed legislation has taken this approach.

²⁵⁵ Amendments to Canada's private sector privacy law (*PIPEDA*) would include protection for prospective employees as well as current ones, but these amendments have only been proposed, not passed. *An Act to Amend the Personal Information Protection and Electronic Documents Act* 41st Parliament, 1st Session. The CRTC, in its New Media hearings in February 2009, online: <<http://www.crtc.gc.ca/eng/archive/2008/n2008-11.htm>>, also looked at regulation of the internet although didn't deal with this question specifically.

²⁵⁶ As of 26 July 2012 Maryland has enacted legislation that prohibits requesting or requiring an employee or applicant to disclose a user name or password for a personal social media account. Delaware enacted legislation prohibiting higher education institutions from requiring students to disclose social media passwords or account information. At least 13 other states have introduced legislation would restrict employers from requesting access to social networking usernames and passwords of applicants, students or employees. See <<http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords.aspx>> for full information. In the Canadian context, Nova Scotia has introduced similar legislation (<http://nslegislature.ca/legc/bills/61st_4th/1st_read/b040.htm>).

Nor does the issue of online searches become moot after an applicant has been hired. *PIPEDA*²⁵⁷ does apply to personal information about an employee of a federal work, undertaking or business, and other jurisdictions may also cover such information under some legal rubric. This is important because, as the US decision discussed above²⁵⁸ shows; online searches may be a tool in disciplinary investigations.

An example of online searches of existing employees resulting in the initiation of disciplinary proceedings is seen in the allegations in the Farm Boy case. Seven (7) Ottawa employees were fired from the chain after the store became aware of the content of their postings on a Farm Boy employee site on Facebook.²⁵⁹ In that situation, a Facebook group called “I Got Farm Boy’d” was set up. The group was set up as a “private” group that didn’t appear in searches, and had only current and former employees as members. Nevertheless, after being told of the forum and postings, Farm Boy terminated 7 of the 186 members of the forum for allegedly making derogatory comments about Farm Boy, its management and its customers. Farm Boy identified this behaviour as contrary to their Code of Conduct in terminating employment.

Recognizing that reputation information is being accessed and used in pre- and post-employment should make it clear why it is necessary to apply legal protections and standards to reputation in order to ensure that only information that is correct and relevant be consulted, and that the individual(s) to whom it refers have awareness of its collection and use as well as of opportunities for challenge, correction and redress where necessary.

²⁵⁷ *PIPEDA* is the *Personal Information Protection and Electronic Documents Act*, the Canadian private-sector privacy law. It will be discussed in more detail in chapter 5; *PIPEDA* S.C. 2000, c. 5., online: <<http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html>>.

²⁵⁸ *Supra* note 251

²⁵⁹ Laura Czekaj, "Workers Fired Over Internet Postings" (7 January 2007) at <http://cnews.canoe.ca/CNEWS/Canada/2007/01/17/3394584-sun.html>.

EDUCATION

Events concerning Ryerson University student Chris Avenir brought to the forefront in Canada the issue of student use of Facebook academically. Avenir faced possible expulsion after being charged with academic misconduct due to his role as an “administrator” of a Facebook group called “Dungeons/Mastering Chemistry Solutions.” This group enabled students to contact each other online regarding homework assignments. Though an administrator of the group, Mr. Avenir, did not post on it. On 18 March 2008, Ryerson ruled that Mr. Avenir would not be expelled, but that the charge of academic misconduct would remain on his record. Though he did ultimately pass the course, Mr. Avenir received 0 on the homework portion of the course (10% of the final mark) and was required to take an academic integrity seminar. Some have suggested that this event is the result of a failure by students to understand that real-world consequences may attach to online activities such as Facebook.²⁶⁰ Others feel instead that the issue is truly one of the failure of the University to properly define parameters of collegial collaboration versus academic misconduct for students, and have encouraged educational institutions to address these issues clearly and in light of current technologies.²⁶¹

Besides academic misconduct, educational institutions have a long history of monitoring SNS for purposes of campus discipline. Recently the University of Calgary has been in Court over its decision to discipline two students over statements they made on Facebook regarding one of their professors.²⁶² Besides disciplining students

²⁶⁰ Shannon Kari, "Facebook Comes to a Head" *National Post* (15 March 2008) at <http://www.oacas.org/news/08/march/15fbbook.pdf>

²⁶¹ Daniel Pagan, "The Line Between Sharing Info and Cheating" *Gauntlet News* (27 March 2008) at <http://www.thegauntlet.ca/story/line-between-sharing-info-and-cheating>

²⁶² In May 2012 the Alberta Court of Appeal ruled that the discipline contravened the students' Charter right to freedom of expression. Canadian Press, "Court sides with two Calgary university students in Facebook free-speech case" *Globe & Mail* (9 May 2012) at <http://www.theglobeandmail.com/news/national/court-sides-with-two-calgary-university-students-in-facebook-free-speech-case/article4105844/>

directly for Facebook utterances, there have also been incidents where colleges and universities monitor Facebook to investigate underage drinking and violations of dry campus policies or discover them while investigating other incidents. For example, several Residence Community Advisors at Northern Kentucky University lost their jobs when pictures were discovered of them having casual drinks in a residence hall one night towards the end of semester.²⁶³

SNS issues have also arisen in student elections, online harassment, and hate speech. Actions have been taken resulting from seemingly suicidal ideations expressed on Facebook profiles, from threats, and even from the perusal of photographs of “illegal” activities to determine those present/involved. In one case, a student who had “humorously” used as his Facebook profile picture a composite police sketch of an alleged rapist was reported to police and arrested.²⁶⁴

Nor is this kind of surveillance restricted to university level institutions. High schools are reportedly perusing SNS profiles as well, in some cases in an attempt to identify alcohol or drug usage, in others to monitor speech. In one case, 5 boys who had created a list rating the Class of 2007 in their school were suspended as a result.²⁶⁵

Finally, there are instances where personal information rather than indicia of behaviour on SNS profiles has been the focus by educational institutions. In two instances where the information indicated the student identified as gay, Christian educational institutions have asked the student to leave their school.²⁶⁶ These issues have, in some ways, been litigated already in Canada. The *Vriend*²⁶⁷ decision made it

²⁶³ Drew Chalfant "Facebook Postings, Photos Incriminate Dorm Party-Goers" *The Northener* (2005-11-02).

²⁶⁴ Y2U. WIKI: Facebook.

²⁶⁵ Don Corrigan, "Does Kirkwood High School Have Jurisdiction Over Off-Campus Internet Activity?" (2006): June 2006 St. Louis Journalism Review 20 online: <<http://www.questia.com/read/1G1-147109993/does-kirkwood-high-school-have-jurisdiction-over-off-campus>>

²⁶⁶ Gretchen Dukowitz, "Out on Myspace, Then Out the Door" (6 June 2006): 964 *The Advocate* online at <http://www.questia.com/read/1G1-147258577/out-on-myspace-then-out-the-door-think-that-no-one> at 22

²⁶⁷ *Vriend v. Alberta*, [1998] 1 S.C.R. 493

clear that a university could not terminate the employment of an individual because of his homosexuality. On the other hand, in *Trinity Western University*²⁶⁸ the Supreme Court of Canada found that the BC College of Teachers could not refuse to allow Trinity Western to undertake a teacher training program simply because students in the program were asked not to engage in “sexual sins” such as homosexuality – the Court felt that there must be freedom to hold beliefs, but cautioned that the freedom to act on them might be more limited. As such, they felt (with Justice L’Heureux-Dube dissenting) that teachers who adhered to such a belief system were not necessarily against the educational good of the province. Finally, in the 2002 Ontario case of *Marc Hall*²⁶⁹, a homosexual student at a Catholic high school sought to bring a male date to the prom. The school tried to prevent him. The Ontario District Court found that since the school was fully funded by the province, it was therefore prohibited from such discrimination by the Charter and human rights legislation.

As with so many other things, there are dual levels operating here. Not only should it be of concern that information is being taken out of context and decisions made based upon it, the impact first of this information and then of the resulting decision upon the reputation of the individual must also be considered. Again, then, it is imperative that the importance of reputation and the relationship between reputation and information be properly understood and protected.

THE COURTS

As in other arenas, both reputation information and identity performances that have been created to facilitate particular reputation(s) are being collected and used in courts as indicia of (un)reliability, veracity and other personal qualities.

²⁶⁸ *Trinity Western University v. College of Teachers*, [2001] 1 S.C.R. 772, 2001 SCC 31

²⁶⁹ *Hall (Litigation Guardian of) v Powers* [2002] O.J. No. 1803 (ON Sup. Ct. J)

In two cases currently proceeding in New Jersey²⁷⁰, a court has ordered the disclosure of emails, diaries and other writings about the eating disorders of two teenage girls. The cases stem from the fact that New Jersey law²⁷¹ requires coverage of mental illness only where the illness is biologically based, which Horizon Blue Cross Blue Shield does not qualify eating disorders as – the insurers refusal to pay for treatment is at issue in the lawsuits. In October 2007 the insurer requested an order for all writings. This was challenged on the ground that writings were therapy tools not meant to be shown to others, and accordingly that forced disclosure could be detrimental to the health of the individuals involved. An order in December 2007 restricted the ordered disclosure to that which had been shared with others, including entries on Web sites such as Facebook or MySpace.²⁷² No decision has been reached in the case, and since legislation is currently pending in New Jersey to explicitly include eating disorders in the insurance coverage, the insurance company has moved to dismiss the case.

Also in New Jersey is an ongoing emotional distress suit²⁷³; a teenage girl was sexually assaulted in 2003 by a fellow middle school student, who has since been convicted. The victim claims that the school's failure to supervise made the attack possible and contributed to her emotional distress. The defence lawyer requested access to the plaintiff's MySpace and Facebook accounts in order to determine the authenticity of her emotional distress. At issue for the judge was the question of whether the privacy features built into SNS confer a different status on this material than emails routed through ISPs, which are discoverable in civil cases. No determination has been made on the matter yet, with the judge ordering the defence to undertake discovery of existing

²⁷⁰ *Beye v. Horizon*, 06-Civ.-5337, and *Foley v. Horizon*, 06-Civ.-6219

²⁷¹ *Mental Health Parity Law* (1999) SB 86 <http://www.njleg.state.nj.us/9899/Bills/PL99/106_.PDF>

²⁷² Mary Pat Gallagher, "MySpace, Facebook Pages Called Key to Eating Disorder Coverage Dispute" (5 Feb 2008) *New Jersey Law Journal* online at: <http://www.law.com/jsp/pa/PubArticlePA.jsp?id=900005502531>. See also Evan Hendricks. "N.J. Blue Cross Subpoenas Teens' Facebook Postings." 2008.

²⁷³ *T.V. v. Union Township Board of Education*, UNN-L-4479-04.

materials and sources before seeking to demonstrate that these additional materials are necessary to the proceedings.²⁷⁴

In Canada many of the cases that examine social media information have been civil situations. Again, however, we see the tension between public and private being played out in these decisions.

In a 2010 case, the court looked to the personal profile information posted on Facebook by the user in order to assess his employment status as either a self-employed contractor or an employee. William Hall testified that while all the other personal information in his profile was true and accurate, his employment status (then listed as self-employed) was not, and that this untruth was a deliberate obfuscation based on privacy concerns. In finding against Mr. Hall, Justice Boyle concluded “that it is not that he lied on Facebook, it is that I do not believe he was telling the truth when he said he was lying on Facebook.”²⁷⁵ No question is raised as to the admissibility of the Facebook profile information here – it is assessed and ultimately forms the basis for the decision.

This is not to say that the admissibility of Facebook data is always unquestioned. Two recent decisions, one in Ontario and one in British Columbia have reviewed the state of the law in the area and come to similar conclusions.

In *Frangione v Vandongen et al.*²⁷⁶ the Ontario Superior Court had the opportunity to review Canadian jurisprudence²⁷⁷ on the question and attempted to formulate an

²⁷⁴Henry Gottlieb, "MySpace, Facebook Privacy Limits Tested in Emotional Distress Suit" (2007):June 7, 2007 New Jersey Law Journal

²⁷⁵ *Shonn's Makeover & Spa v M.N.R.* [2010] TCC 542 (Can Lii) <<http://canlii.ca/t/2d7g3>> at para 29.

²⁷⁶ *Supra* note 242

²⁷⁷ There were a series of cases, primarily from Ontario, that had examined the relationship between Facebook posts and the rules of discovery in civil suits. In *Murphy v. Perger*, [2007] O.J. No. 5511 (Sup. Ct), the plaintiff had posted pictures of himself enjoying various activities – the court ordered the disclosure not only of the relevant information but of the entire profile. A number of cases in 2009 also explored the issue. At the NB Court of Queen's Bench, in *Carter v Connors* (2009) NBQB 317 the request was made for

approach. Two (2) major points are extrapolated from this review: (1) that it is accepted that a person's Facebook profile may well contain information that is relevant to a proceeding; and (2) that even when dealing with a profile that has been limited using privacy tools, it is still appropriate for the court to extrapolate from the nature of the social media service that relevant information may be present.²⁷⁸

Similarly, in British Columbia's *Fric v. Gershman*²⁷⁹, after reviewing the British Columbia and Ontario jurisprudence (though not, interestingly, Frangione), Master Bouck concluded that information from a private Facebook profile should be produced. This decision was grounded in three conclusions: (1) that the existence of a public profile implied the existence of a private profile that could contain relevant²⁸⁰

production of the plaintiff's internet usage records, including Facebook, from her ISP. In considering it, the judge was of the opinion that the potential probative value of the information was high and that the information was of a type in which the plaintiff could not have had a reasonable expectation of privacy. In contrast to these cases where full disclosure of the Facebook profile was ordered, a trio of Ontario Superior Court decisions nuanced the relevance question. In *Wice v Dominion Insurance of Canada* (2009) CanLii 36310 (ON Sup. Ct) <<http://canlii.ca/t/24j5t>>, the court ordered the preservation of the Facebook profile, but required only that plaintiff file a new Affidavit of Documents listing relevant information from the Facebook profile. Similarly, in *Leduc v Roman* (2009) CanLii 6838 (ON Sup. Ct) the court considered this question in relation not simply to a (publicly available) Facebook profile but rather information that was on a Facebook profile with privacy settings restricting access to friends only. There, the court stated at para 32 that "a party who maintains a private or limited access Facebook profile stands in no different position than one who sets up a publicly available profile." Further, the court concludes that despite the privacy settings on the profile, given the social networking focus of Facebook and the information sharing applications available to users it was legitimate to infer that information was intended to be public, and that it was similarly reasonable to infer that some documents on the profile would be relevant to the issue. This did not result in the disclosure of the entire Facebook profile, but the plaintiff was required to submit to cross-examination regarding the profile in order to allow the defendant to identify any information that might be relevant. Finally, in *Schuster v Royal & Sun Alliance Insurance Company* (2009) CanLii 58971 (ON Sup Ct.) <<http://canlii.ca/t/26cv5>> the insurance company sought an interim order preserving the plaintiff's Facebook page, but the court did not agree. Instead, and in common with *Leduc*, they ordered that the plaintiff submit to cross-examination on her Affidavit of Documents.

²⁷⁸ *Supra* note 242 at paras 34-35

²⁷⁹ (2012) BCSC 614

²⁸⁰ Interestingly, despite the fact that discovery rules do not apply to third parties, a recent Quebec court decision in <*Landry c. Provigo Québec Inc (Maxi & Cie)*>, 2011 QCCLP 1802 (CanLII) considered the Facebook posts of 3d parties. The employer in that case raised the question of the privacy interests of the third

information; (2) that since the plaintiff was relying on photographs of her prior to the accident it was only fair that the defendant have access to photographs after the accident; and (3) that the fact that the profile was limited to friends was somewhat irrelevant given that she had over 350 “friends”, thus suggesting publicness.

Courts, then, have tended to allow information from social media profiles – regardless of whether privacy settings have been used or not – to be disclosed as relevant to assessment of mobility, recreation abilities and pursuits, social interactions and engagements, ability to work and even quality of life questions.

Indeed, lawyers in are increasingly finding that SNS contain “treasure chests of information”²⁸¹ useful in both civil and criminal proceedings. Pictures, comments, texts and even social connections demonstrated by these sites have been submitted in court as evidence. John Palfrey of the Berkman Center for Internet & Society at Harvard Law School cautions that because SNS are so new, there are not many precedents about the admissibility of information from SNS in court. He indicates, however, that judges seem to be suggesting that this information will be treated like any other electronic evidence, meaning that the focus will be on authenticating what was said and who said it rather than a consideration of the context(s) in which it was said or created.²⁸² It is unfortunate that context may not be considered when weighing admissibility of SNS information. Jesse Hirsch was accepted as a “Facebook Expert” in the Ontario criminal trial of a young man who posted comments on his Facebook threatening a suicide attack against the Children’s Aid Society who had recently apprehended his infant son. Hirsch testified that Facebook users “routinely embellish what they say as part of an online persona.”²⁸³ Alas, unless lawyers understand the importance of context and

parties, but consistent with the caselaw already reviewed, the court decided that the parties did not have a reasonable expectation of privacy in their Facebook posts.

²⁸¹ Vesna Jaksic “Litigation Clues are Found on Facebook” *National Law Journal*. 15 October 2007. <http://vesnajaksic.com/?page_id=35>

²⁸² *Ibid*

²⁸³ Shannon Kari, “Facebook Comes to a Head” *National Post* (2008). *Supra* note 61.

press courts insisting on the right to lead evidence contextualizing the posts admitted into evidence, such testimony is unlikely to be received or applied. The lack of this information, combined with uncertainty about accuracy or relevance should be of concern when such information is admitted into court.

LAW ENFORCEMENT

Just as campus authorities and lawyers are turning to SNS for information and evidence in investigations and proceedings, so too are law enforcement bodies reviewing the sites. Indeed, the use of SNS information is increasingly ubiquitous in law enforcement activities in a variety of ways, so much so that documenting or discussing it almost seems redundant. It must be of just as much concern, if not more, to have reputation and identity performances in aid of particular reputation(s) be used by law enforcement in arenas far beyond their original intent or derivation.

A Lexis Nexis Risk Solutions 2012 survey of 1200 law enforcement professionals reveals the extent to which social media use has permeated law enforcement activities. At least 50% of the respondents use social media at least weekly for law enforcement purposes, and 67% believe that social media use is of assistance not only in solving crimes but in solving them quickly. The study shows that social media information and platforms are used for a variety of purposes, including identifying persons, discovering criminal activity in the first place, and gathering evidence.²⁸⁴

Research on social media conducted for Public Safety Canada recently included 11 interviews with persons related to law enforcement about their use of social media in February and March 2011. In their results detailing the way(s) in which social media may be used in information gathering and investigations, respondents discussed Open Source Intelligence gathering (OSINT).

²⁸⁴ Lexis-Nexis: News Release, Role of Social Media in Law Enforcement Significant and Growing; 18 July 2012 <<http://www.lexisnexis.com/media/press-release.aspx?id=1342623085481181>>

Taken together, the respondents painted a picture of a typical OSINT gathering exercise. First an individual or group of individuals (suspect) is identified. The suspect's profile is sought on multiple OSMS in hopes that the suspect is available on at least one. The suspect's network of friends, co-workers, collaborators and relatives is built based on his linkages to other individuals or groups (including gangs) on OSMS. At the same time, information specific to the suspect is collected, such as phone numbers, age, aliases, city, and nearest intersection or addresses frequented. This information can be derived from GPS coordinates embedded in photographs, for instance. Some individuals make this information private on the OSMS they frequent. Police and private investigators can attempt to befriend such individuals using fake accounts in order to try to infiltrate the network of the suspect. Fake accounts can be long-term efforts with the goal of gaining enough connections with the suspect to earn their trust. Once sufficient information about the suspect is collected, the individual or members of the network can be charged by law enforcement.²⁸⁵

This approach, of course, is used to collect information about an already identified suspect. While this may have a positive impact in some cases such as that of Rodney Bradford, who was being investigated for armed robbery and was exonerated by a Facebook status,²⁸⁶ there is still a large collection of personal information and the inferences drawn at issue, including reputation information in its own right as well as that which is tied to reputation through performance or social connection(s) to others.

There are also instances where law enforcement are aware of a particular incident and are able to use social networks in order to identify a suspect. In both the Vancouver, BC, Stanley Cup riot and the London, Ontario, riots, law enforcement interacted with SNSs in novel ways. While participants were posting pictures and stories on Facebook,

²⁸⁵ Dr. Richard Frank et al., "Social Media Sites: New Fora for Criminal, Communication and Investigation Opportunities" Public Safety Canada online: <<http://www.sfu.ca/icrc/content/PS-SP-socialmedia.pdf>> at 12.

²⁸⁶ Colin Miller "Facebook Status -- Exonerated: Suspect's Facebook Update Corroborates Alibi In Brooklyn Robbery" (13 November 2009)Evidence Prof Blog online at <<http://lawprofessors.typepad.com/evidenceprof/2009/11/i-have-written-several-posts-on-this-blog-herehereherehere-andhere-about-cases-dealing-with-the-admissibility-of-eviden.html>>

Twitter and other networks, police were able to follow the action, identify perpetrators, and levy charges more serious than simple participation (in the cases of those who detailed their actions).²⁸⁷ It is interesting to note as well that SNSs can be used for law enforcement purposes by those other than law enforcement agents; in the wake of the Vancouver riots especially, numerous Facebook groups were set up by users for the purposes of assisting with identifying perpetrators.²⁸⁸ Others eschewed Facebook and used the web directly to set up similar sites.²⁸⁹

Law enforcement does not simply use SNSs as part of the investigation into an incident; rather, it is increasingly the case that an SNS is monitored proactively, as in the case of the NYPD, who actually set up a Facebook team to monitor SNSs on an ongoing basis,²⁹⁰ or the recent revelation of the Department of Homeland Security's *Analyst's Desktop Monitor*,²⁹¹ that included a list of key words and search terms that are monitored prophylactically for security reasons.

STATE

An internal Department of National Defence memo indicates that the Canadian military is warning soldiers not to post personal information on SNSs due to national security concerns.²⁹²

Aric Hanson, on the other hand, suggests that the military in both Canada and the United States monitor SNSs for reasons beyond those of national security. His research

²⁸⁷ Taylor Scott, "Social Media Valuable Source for Police" *London Free Press* (9 August 2012).

²⁸⁸ See for example: Vancouver Riot Pics: Post Your Photos, online: <<https://www.facebook.com/vancouverriot2011photos>>.

²⁸⁹ Identify the Rioters: <<http://www.identifyrioters.com/>>.

²⁹⁰ Clay Dillow "NYPD Creates Facebook-Police Taskforce to Mine Social Media for Clues" *PopSci* (2011) online: <http://www.popsci.com/technology/article/2011-08/nypds-facebook-police-mine-social-media-clues-about-crime>

²⁹¹ US Department of Homeland Security. *Analysts Desktop Binder*. Media Monitoring Capability Desktop Reference Binder. (2011) <<http://www.scribd.com/doc/82701103/Analyst-Desktop-Binder-REDACTED>>

²⁹² Jeremy Barker, "Facebooking With the Enemy" (2008) online at <http://www.oacas.org/news/08/feb/26fbbooking.pdf>

indicates that especially under the US's Don't Ask, Don't Tell policy²⁹³, soldiers with SNS profiles that indicate their homosexuality (or even seemingly call into question their heterosexuality) may become subject to investigation and eventual discipline and dismissal from the military.²⁹⁴

Outside the military, it was recently revealed that the BC Ministry of Employment and Income Assistance (who provide welfare assistance) and the Ministry of Children and Families are using Facebook, MySpace and other public domains in order to search for evidence of: undisclosed co-habitation; spending beyond what is provided by the Ministry; casual employment; leaving the province for more than 30 days; or gifts, pets and other income.²⁹⁵ Given that it is extremely unlikely that such searches are engaged only in a search for explicit statements to these effects, it is the inferences drawn from information rather than statements themselves that are most likely at issue. Removing information from its SNS context and using inferences drawn from it to affect the most basic livelihoods and entitlements of individuals. This is extremely troubling.²⁹⁶

In the Netherlands it has been revealed that tax inspectors have been searching SNSs (specifically Facebook), seeking to collect information about individuals for the purposes of audit investigations. A spokesperson for the agency responded that there was no specific policy decision in place to use SNSs, but rather that auditors would use

²⁹³ Don't Ask, Don't Tell (DADT) was created by US federal Law Pub.L. 103-160 (10 U.S.C. §654). The law barred openly gay, lesbian or bisexual persons from entering the military or undertaking military service. The focus on "openly" meant that (a) harassment or discrimination against GLB persons who were not out was prohibited and (b) evidence of open homosexual behaviour was required before supervisors could initiate an investigation. DADT ended 20 September 2011.

²⁹⁴ Aric Hanson, "Don't Ask, Don't Tell, Don't Blog, Don't Enlist: How the Internet Has Affected the Military's Policy on Gays and Lesbians" (2007).

²⁹⁵ Public Service Alliance of Canada, BC, "The Facebook Trap!" (2007) online: <http://wp.psacbc.com/2007/11/30/the-facebook-trap/>

²⁹⁶ Murray Long, *Privacy Scan* (special issue) 2008

any sources of information that are publicly available to them in preparation for an audit.²⁹⁷

Yet again, then, we see the use of reputation information as well as identity performances intended for reputation derivation being collected and used in another context and for a variety of purposes – to assess individual's 'worthiness' for benefits, to ensure compliance with expectations outside those of the job, etc.

Information Analysis

In each of the categories discussed above, we see information; reputation information, reputation-related information about social connections, and identity performances - that are intended to facilitate reputation assessments- which is removed from its context and analysed for third party purposes. This is the sort of situation flagged by Nissenbaum when she talks about the way information technologies are revealing flaws in the categorical public/private divide. With SNS information, there are the issues identified by boyd, those of persistence and searchability. This makes the situation categorically different than the traditional understanding of utterances in public. Information in online spaces is not ephemeral and may be re-viewed out of context and in perpetuity. Thus, rather than understanding the information as part of identity performance in reference to specific normative values in a given context, information is decontextualized and (mis)understood at face value, orphaned from the context which could explain or situate it.

Denial of Access

The issue with (mis)use of reputational data is not restricted to third party access to or use of the information; just as particular identities are developed and performed in order to create desired impressions and thus gain access to social approval, so too may the inferences drawn from particular pieces of information or even the overall

²⁹⁷"Taxman Admits to Facebook Trawl" The Independent (25 February 2008) online at: <http://www.independent.ie/national-news/taxman-admits-to-facebook-trawl-1297118.html>

reputation derived from such performances function to deny access to information and even participation in certain arenas. In each of the areas already referred to – employment, education, courts, law enforcement and the State – we have seen examples not only of information being accessed, but of that information and the inferences derived from it being used to grant or deny access to particular arenas. Reliance upon this information, when the information is inherently a social artefact, created and re-created in social situations and for particular purposes is problematic; enforcing and reinforcing particular normative expectations and thus privileging certain groups or communities. Consulted in pre-employment and employment situations, reputation information has the possibility to prevent or restrict securing employment as well as grounding the imposition of restrictions on existing employees. Similarly, in education there were various academic penalties (suspensions, discipline, etc.) that were the result of this process. Effectively, the reputational information came to function to deny its subject access in some way; access to the right to attend an institution or some other form of restriction on participation within, and access to, the resources of the education system. Courts and law enforcement use of such information has resulted in acquittals and convictions within the criminal justice system (perhaps the most basic example of how such information becomes a key to either freedom or to restriction thereof) as well as civil processes. State collection, derivation and use of reputational information has been shown to impact an individual's ability to access basic State resources and thus to restrict basic subsistence.

danah boyd relates a story of being contacted by the admissions officer for a university. The school had intended to offer admission to a particular inner-city applicant whose essay had been extremely critical of gangs and gang culture. Given this, the admissions officer was dismayed on reviewing the applicant's SNS profile, to find it rife with gang inferences and language. Boyd was able to offer an alternate reading of the seeming conflict, suggesting that rather than the application essay being inauthentic and the profile presumptively representative, the profile might instead simply reflect the necessity of acquiescing to neighbourhood norms in order to survive. Reflecting on this, she writes that:

...situations like this highlight how context is constructed and maintained through participation, not simply observation. When outsiders search for and locate participants, they are ill prepared to understand the context: instead, they project the context in which they relate to the individual offline onto the individual in this new online space.²⁹⁸

This anecdote raises various issues of concern, as well as demonstrating the way(s) that particular assumptions – in this case, around racialized youth and gang activity – can be embedded into identity performance and (mis)understood.

First, it emphasizes (again) the importance of context in understanding reputation, social interactions, and identity performance(s). As we see more and greater online participation as well as the collection and data-mining of personal information and identity performances from those spaces, it is impossible to overstate the importance of context in understanding them. Notice here that it is not just the actual reputation or performance that is at issue here but also the inferences that are or may be drawn from that information. Presentations, connections and interactions are informed by the context in which they exist, as well as existing for the purpose of facilitating interactions and social capital within those spaces.

Additionally, at least arguably, the issue here is not merely the decontextualization of the information, but access to the information in the first place. I discussed earlier the legislative discussions about protecting social network passwords so that employers cannot require prospective employees to provide them, and noted that this does not in fact solve the issue. The issue isn't about protecting the passwords from prospective employers, but rather about protecting the actual information itself. Similarly here, while boyd was able to contextualize the information for the admissions office in a way

²⁹⁸ danah boyd "Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life." In *Youth, Identity and Digital Media*, edited by David Buckingham, MacArthur Foundation Series on Digital Learning (2007) at 17

that was palatable to them, the larger issue must be about the appropriateness of the admissions office accessing the applicant's SNS profile in the first place. As discussed in chapter 3, SNS profiles are exercises in identity definition and performance within a particular space and for a particular audience. Understood that way, there is a dissonance in the notion that such a profile could or would be at all relevant to a college/university application.

boyd's story shows the importance of fully understanding the issue, of understanding the way performances are socially influenced and constructed, as well as how they may be interpreted, and reinterpreted, until the social actor becomes defined by the meaning(s) attributed to the performance in the first place.²⁹⁹

It also shows the way that reputation or reputation-related information may not only be collected, but may effectively prevent its subject from accessing services, communities or information whether it is understood in context or not. In this case, of course, context definitely played a role in the access analysis; when the inferences drawn by the admissions office did not match with the admissions essay submitted with the student's application, the student would have been denied access to the university but for boyd's ability to contextualize the information for the admissions officer. It is important to consider, however, not simply the need for context, but also whether that need should ever have arisen; should access to the student's SNS page have been available to the admissions office at all? Why is it presumed that the information provided on the SNS is more or less reliable than that provided on the admissions essay? Why should a student with gang affiliations be considered less acceptable for admissions if all other standards are met, and what assumptions about race and class might factor into that consideration?

Nissenbaum discusses what she calls transmission principles; constraints that govern the way information flows (the collection, use, or disclosure of personal information),

²⁹⁹ Valerie Steeves, personal communication (20 November 2012).

between parties in a given situation.³⁰⁰ This gets at a new way of understanding information relationships; a nuanced management of information flow rather than the application of categories of “shareable” or “protected” to information, after which the flows are uncontrolled where allowed. While Nissenbaum talks about “transmission”, David Lyon builds on Bauman’s liquid modernity to look at fluidity in surveillance, describing how:

... the sense of flow becomes palpable as personal information moves constantly from the individual to the database and back again, via experiences of access and denial, inclusion and exclusion, privileges, rewards and benefits or lack thereof. The individual is unlikely to have a sense that drinking at a particular bar may reduce chances of obtaining credit or that cross-border shopping may attract the interest of officials in an unemployment benefit department. However, the commercial information about visits to the bar may be traded such that institutions concerned with credit-worthiness or the likelihood that credit card debts will be repaid on time may use them to situate the consumer within a category of risk...³⁰¹

Gatekeeper theory was first articulated by Karl Lewin³⁰², and refers to the process by which decisions are made about whether information should be shared with a group/individual or whether it should not be shared. It is imperative to make the distinction here between a gate (passive object) and a gatekeeper (an active process). A gatekeeper is necessarily exercising a role that incorporates and reaffirms chosen social, political, and cultural norms.

Just as norms and risk analysis were shown to be integral to trust derivation, which in turn led to a willingness (or not) to assume risk, so too in the case of gatekeeping does information, the inferences drawn from it, and a given reputation or conception of an

³⁰⁰ Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Palo Alto, Stanford University Press, 2009) at 145.

³⁰¹ David Lyon, “Liquid Surveillance: The Contribution of Zygmunt Bauman to Surveillance Studies” *International Political Sociology* (2010) 4 325-338 at 331

³⁰² K. Lewin(1943) *Psychological Ecology in Field Theory In Social Sciences I* (New York: Harpers 1951)

individual, function as an integral part of the process, effectively acting as a signifier that weights heavily towards information sharing or refusal. In a society and economy that is increasingly information-saturated, an inability to access particular information, services or communities can have devastating effects.

Maria Los writes that, “[i]n the absence of clear rules, institutional guarantees, or a rationality-based political culture, each individual almost instinctively marks for him or herself the taboo areas to avoid. The world of ordinary people becomes structured through a series of such taboos involving subjects, spaces, behaviours, gestures, words and persons.³⁰³ There is a web of gatekeeping and analysis taking place here; communities develop norms and values, and individuals within communities develop an understanding of areas to avoid and social negotiations to facilitate those pursuits. Social processes become increasingly shaped by these taboos and expectations, which themselves become self-reinforcing.

Managing Reputation

On Data Privacy Day 2012, Microsoft released a study about online reputation management. The study looked at two groups; – adults, and children between the ages of 8-17 from the US, Germany, Ireland, Spain and Canada. Among other findings, the study indicated that a majority (67% of adults and 73% of children) report feeling in control of their online profiles, yet conversely it appeared that participants mis-weighted the relevance of information, for instance ranking SNS information as only the 4th most important contributor to online profile, rather than the most important, as Microsoft’s research indicated it to be. In a similar contradiction, despite indicating an awareness of the impact of the online postings on both their own reputations and those of others, study participants nevertheless tended to identify their online participation

³⁰³ Maria Los, “The Technologies of Total Domination” *Surveillance & Society* 2(1): 15-38, online: <<http://www.surveillance-and-society.org>> at 28.

as primarily having a neutral or even positive impact on their online profile, a fact not born out in practice.³⁰⁴

Solove wrote that:

Everyone must cope with the fragility of reputation, on which the ability to function in society delicately hangs. All who value their reputations care about how others judge them. Reputation is especially important in one's public roles, because these roles shape one's career, relationship with much of society, participation in political life, and financial well-being. The reality is that people lack much control over how they are judged. One is constantly at the mercy of others – a precarious position to be in. However, managing disclosures about one's private life is an even greater and more difficult burden, making reputation all the more vulnerable.³⁰⁵

With the introduction of both context and Nissenbaum's transmission theory, the discussion of informational norms transforms from one about "control" to a far more nuanced project, one that determines what is appropriate with reference to "the context, the types of information, the subject, sender and recipient."³⁰⁶

The Microsoft survey shows a disconnected understanding of informational norms and transmissions. In some ways, even the focus of the study is off target, focussing on an understanding of the implications of information put online by individuals themselves. Throughout these first 4 chapters, however, I have been at pains to demonstrate the chasm between individuals and their information. That is, individuals put information online in particular contexts and to achieve particular ends of identity performance and definition. On some level, however, this is all performance *for* rather than performance *by*, that is, it is what other people do with that information that is ultimately at issue. Information can be selected by an individual and targeted towards desired ends, but

³⁰⁴ Microsoft, "Online Reputation Management Survey" Data Privacy Day 2012, online:

<<http://go.microsoft.com/?linkid=9797152>>.

³⁰⁵ Daniel Solove, "The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure" at 1039

³⁰⁶ Helen Nissenbaum, *Privacy in Context* at 148.

how it is interpreted is governed at least in part by those who see that information. Identities are developed and performed in online spaces, but again the identity we claim must be validated by those for whom we perform it in order to be perceived as authentic.

There is then a dual recognition; first, that reputation writ large impacts our access to services, spaces and information; and second, that an individual cannot effectively control their reputation since it is at least in part a product of the application of norms and assessment of information by others. Building on these recognitions, I will now proceed to an examination of the expectations about, and current remedies for, reputation damage in the second part of this dissertation.

CHAPTER 5: Existing Legal Frameworks for Reputational Governance

In this dissertation, I have taken on the role of the under-labourer, seeking to ground and focus the inquiry into whether and how reputation issues should be regulated. This project itself breaks down into two (2) parts.

Part I of this dissertation was comprised of four (4) chapters, and sought to fully examine the idea of reputation in order to assist with a properly focussed and informed analysis on the question of regulation.

In Chapters 1-3, I explored the concepts of “identity”, “reputation” and “trust”, showing them to be interrelated issues that may be discussed under the rubric of reputation. That is, information that is provided by an individual constitutes an identity performance. Thus, a reputation is a social artefact, incorporating both the information provided by an individual, her identity performances in which that information is implicated; the inferences drawn by others from that information; and the overall assessment that others make and share from the analysis of the information and inferences weighed against socially constructed expectations.

In chapter 4, having grounded those terms, I moved to a discussion of how reputation information is used; how third parties form impressions, collect and use performances intended for a particular audience, and repurpose that information. Having shown reputation information to be socially produced and contextual, that chapter then moved to examine how the use of that de-contextualized information, performances intended for reputation support, and reputations derived from it in turn become implicated in a *de facto* gatekeeping process, facilitating or acting to deny access to information, community participation, and services.

The focus shifts now in Part II to look at the question of how and whether such complex social systems can or should be regulated. Looking at a variety of avenues, including public perceptions, policy analyses and existing legal approaches, I will attempt to explore regulation and remedy for reputation injuries, at both the individual and community levels.

To begin, I will examine the way(s) in which participation and (mis)use of reputations are or may already be being regulated by existing institutions.

Scope of Harm

As discussed in Part I of this dissertation, reputation has resonance and meaning in a variety of different avenues. Despite this, the traditional private law approach to reputation is predicated on the ideas of harm and damage, requiring that harm be established in order for a claim to be successfully made out. That is, in order to address, it is important to first consider what the value of reputation really is, or put another way, what (quantifiable) harm follows from reputational injury.

Friedman notes that reputation has economic impact³⁰⁷ and this is certainly true; career progression, employment consequences, and business success³⁰⁸ may all be impacted by the lack of a good reputation or by injury dealt to an individual's reputation. However, while Friedman seeks to extend the analysis of reputation beyond its social impacts and quantify it, I believe this approach to be inadequate for dealing with the full import of reputation and reputational damage.

³⁰⁷ Lawrence M. Friedman, *Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety and Privacy* (Stanford: Stanford University Press, 2007) at 3

³⁰⁸ Elad Peled, "Should States Have a Legal Right to Reputation? Applying the Rationales of Defamation Law to the International Arena" (2010) 35:1 Brooklyn Journal of International Law. It is also worth noting that these same areas where reputation impacts are the very areas identified in Chapter 4 as arenas that can and have accessed (and used in decision making) personal information from online spaces and sites.

In his germinal text on defamation, Brown argues for an understanding of reputation that transcends the merely economic, writing that:

...it is universally recognized that the reputation of a person is, and always has been, an important value which the law must protect. Some form of legal or social constraints on defamatory publications “are to be found in all stages of civilization, however imperfect, remote and proximate to barbarism.”³⁰⁹ The extent to which a community protects the reputation of its citizens may partially measure its cultural level and democratic quality.³¹⁰

Indeed, some of the earliest writings on reputation have focussed on how reputational damage may effectively impair “a person in the enjoyment of general society and injuring rights of friendly intercourse and mutual benevolence, which man has with respect to men.”³¹¹

This kind of thinking, an understanding of reputation that transcends the economic and instead focuses on issues of dignity and autonomy, is consistent with International and Canadian jurisprudence as well.

Internationally, rights instruments such as the UN Declaration of Human Rights Article 12³¹² recognize the right to protection of reputation; and in Canada, Justice Cory, writing for the majority of the Supreme Court of Canada, recognized after a survey of literature on the matter that: “[a]lthough it is not specifically mentioned in the Charter, the good reputation of the individual represents and reflects the innate dignity of the individual, a concept which underlies all the Charter rights. It follows that the protection of the good reputation of an individual is of fundamental importance to our

³⁰⁹ Henry Coleman Folkard, *The Law of Slander and Libel*, 5 ed. (1891) at 7

³¹⁰ Raymond E. Brown, *The Law of Defamation in Canada*, vol. 1 (1987) at 4

³¹¹ Lawrence M. Friedman, *Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety and Privacy* (Stanford: Stanford University Press, 2007) citing Francis Holt at 41

³¹² UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III), available at: <http://www.unhcr.org/refworld/docid/3ae6b3712c.html> [accessed 15 December 2012]. Article 12

democratic society."³¹³The human rights approach, however, may not be sufficient to address the full complexity of reputation.

Julie Cohen, in the introduction to *Configuring the Networked Self*, argues that:

Human being and human societies are constituted by webs of cultural and material connections. Our beliefs, goals, and capabilities are shaped by the cultural products that we encounter, the tools that we use, and the framing expectations of social institutions....The legal, technical, and institutional conditions that shape flows of information to, from and about us are of the utmost importance not because they promote free speech or free choice in markets, but because they shape the sort of subjectivity that we can attain, the kinds of innovation that we can produce, and the opportunities for creation of political and ethical meaning that we can claim to offer.³¹⁴

Reputation is a social artefact, produced with reference to social norms and values, and both regulates and is regulated by those socially negotiated and agreed upon standards. At issue here, however, is the question of whether this kind of social self-regulation and co-regulation is sufficient, or whether, given the importance of reputation, there should be some kind of regulatory authority created. This could take a variety of forms, essentially some form of law to support claims or a body to which appeal may be directed (in case(s) of unfairness, fraud, error, or unjust injury or enrichment) or even perhaps which functions simply as a normative background and reference point. Having dual regulatory functions – legal and extra-legal – is not a novel approach but a complementary one.

In this exploration of reputation and its regulation, the next step is to look at existing legal instruments and assess whether they are capable of encompassing the full import of reputation in contemporary society; that it is “central to social, political and

³¹³ *Hill v. Church of Scientology of Toronto* [1995], 2 S.C.R. 1130 at para. 120

³¹⁴ Julie E. Cohen (2012) *Configuring the Networked Self: Law, Code and the Play of Everyday Practice* (Yale University Press: New Haven) at 5.

economic relations”³¹⁵ with its links to civilization and social contracts, economic opportunity, human dignity and subjectivity. To focus solely, or even primarily, on economic damage, quantifiable harm or any other single factor is to diminish both the harm(s) suffered and the importance of reputation.³¹⁶

I shall proceed, then, to examine the current legal approaches and regimes that might be applied to reputation in order to assess whether each is, or could be, an appropriate way to address the issue of reputation protection.

Current Legal Approach: *Criminal Code*

The *Criminal Code of Canada* is one potential regime under which reputation might fall, accordingly, the way(s) in which it does or doesn’t cover reputation must be assessed.

The Code doesn’t speak specifically of reputation, but does recognize three different types of libel. Seditious libel, set out in s. 59(2); blasphemous libel, set out in s. 296(1); and defamatory libel, set out in s. 298. Although possible, it is unlikely that sedition or blasphemy will be applicable; seditious libel primarily protects the state and thus is focussed more on political viability than on relationships between persons, and blasphemous libel is a historical anachronism and unlikely to survive a Charter challenge.

Defamatory libel as set out in s. 298 is a different matter. At first blush it can be used to regulate online communications and harms to online reputation, however it is limited by a number of factors.

³¹⁵ Valerie Steeves, personal communication (28 November 2012).

³¹⁶ It is for this reason that this paper will not deal with laws of trademarks or copyright. While an argument may be—and has been – made that the focus on an individual “brand” in online spaces lends itself to such analyses, it is the opinion of this author that those forms of law are rooted in economic rather than rights protections, and accordingly are inherently inapplicable and insufficient to properly address the issue of reputation harm.

298. (1) A defamatory libel is matter published, without lawful justification or excuse, that is likely to injure the reputation of any person by exposing him to hatred, contempt or ridicule, or that is designed to insult the person of or concerning whom it is published.

(2) A defamatory libel may be expressed directly or by insinuation or irony

(a) in words legibly marked on any substance; or

(b) by any object signifying a defamatory libel otherwise than by words.

299. A person publishes a libel when he

(a) exhibits it in public;

(b) causes it to be read or seen; or

(c) shows or delivers it, or causes it to be shown or delivered, with intent that it should be read or seen by the person whom it defames or by any other person.³¹⁷

Defamatory libel is defined as something “published, without lawful justification or excuse, that is likely to injure the reputation of any person by exposing him to hatred, contempt or ridicule, or that is designed to insult the person of or concerning whom it is published.” In order to assess the applicability and efficiency of this section in dealing with reputation systems, we will need to parse the offence.

First, the question of publication: Section 299 of the *Criminal Code* defines publishing relatively broadly, stipulating that a libel is held to be published when it is (a) exhibited in public; (b) caused to be read or seen; or (c) shown or delivered or caused to be shown or delivered with the intent that it be read or seen by the person to whom it relates or by any other person. This question of “publishing” already demonstrates hurdles for the application of the *Criminal Code* to reputation. As we have seen, reputation systems may have multiple levels; both the individual comments/assessments, and then an overarching meta-reputation or aggregate reputation in which the individual feedback is subsumed. Where the individual

³¹⁷*Criminal Code of Canada* R.S.C. 1985, c. C-46

comments are visible in some way, this would seem to be sufficient to meet the definition of publication. The larger problem with reputation systems, however, is that aggregate score, and its impact both on future individual assessments and on access to services. Where the aggregate score is available – as in a formal reputation system – then it too would appear to meet the definition of publication.

Separate from publication is expression; a defamatory libel must be expressed. Section 298(2), however, provides an expansive definition that includes both direct statement and statements that give rise to defamatory inferences, as well as recognizing both words and symbols as sufficient. In those circumstances it seems there is very little likelihood that individual comments as well as aggregate scores or other representations would not be found to be expressions within the scope of the section.

Next, the publication must be without lawful justification or excuse. It is noteworthy that of the three libels recognized in the *Criminal Code*, only this one contains within it the possible defences of justification and/or truth. Lawful justification or excuse is covered in s. 304-316, which codify the possible defences to the charge of defamatory libel; (1) selling a book containing a libel; (2) publishing the proceedings of the court; (3) publishing under the auspices of or for the benefit of Parliament; (4) good faith reporting of Parliamentary; (5) judicial (except divorce); (6) public meeting proceedings; (7) public interest revelation of information believed to be true; (8) fair comment on public persons or works; (9) establishment of the truth of the statement(s); and (10) publication that is invited, necessary or required.

I have concerns about whether this provision or these defences would apply to reputation. When looking at fair comment, for instance, we must question whether an individual interacting on a particular site or within a particular community (on- or off-line) is indeed a public person and whether those actions are indeed public ones.³¹⁸

³¹⁸ There is a common belief that participation in online spaces makes information presumptively public. It is noteworthy, however, that this reasoning tends to be applied to all sites and communities online

Similarly, given the inherently subjective and performative nature of many of the statements, perceptions, and presentations from which reputations are derived, it is difficult to see how truth as a defence could be established with any certainty.

Finally, there is the question of whether the publication was either likely to injure or designed to insult. Section 300 prescribes penalties for an offender who publishes a libel known to be false, but since s. 301 deals more generally with punishment for publication of a defamatory libel, it is clear that the section is intended to address situations beyond those of a known falsehood. Where the other aspects of the offence have been grounded, this will require demonstration of the intent to publish the material alleged to be defamatory. For individual reviews/assessments (leaving aside issues of anonymity and pseudonymity) this should not be difficult to establish, but it is difficult to imagine how the necessary *mens rea* could be found to exist in, for instance, an algorithm that combines scores or assessments to create the aggregate or overarching indicator.³¹⁹

Arguably, then, the *Criminal Code* offence of defamatory libel could apply in many (if not all) cases of reputational harm. The fact that it can, however, does not necessarily mean that it should, or that it is the most effective way to address the problem.

regardless of whether those sites require membership, agreement to a Terms of Use that restricts what uses may be made of information within the space, or other limiting features. Similar arguments could be made about information that is released within offline communities – there mere fact that they take place among other persons should not be taken as automatic indicia of publicness, since again there are communities and spaces that carry with them presumptions of privateness or at least of limited audience.

³¹⁹ Difficult to imagine, perhaps, but not impossible as shown by a recent French court decision which found that Google Search autocorrect suggestions (which are derived by an algorithm which identifies the most common searches performed by other Google users associated with the text already typed into the search) did constitute defamation and fined Google \$65,000. <<http://www.webpronews.com/google-fined-65k-for-defaming-search-suggestion-2011-12>>. See as well John Gregory "Can a Google Search Suggestion Be Defamatory?" (2012). A recent Australian case looked at a similar issue <<http://www.austlii.edu.au/cgi-bin/sinodisp/au/cases/vic/VSC/2012/533.html?stem=0&synonyms=0&query=trkulja>>.

First of all, the problem with using the criminal law system for redress is that, to a great extent, it is out of the hands of the individual who has been harmed. While she can report the violation to the police, what happens from there is in the hands of law enforcement and the Crown; the investigation, the decision about whether to prosecute, even the identification of the damage. There is no guarantee that reputational damage will be prosecuted under the *Criminal Code*, only the possibility of it being done.³²⁰

In addition, there is the question of scope. This appears to function in two ways. First of all, although I have demonstrated the role of reputation not just socially but in terms of access to services and knowledge – an important, if not integral access in these times – many of the reputation harms would not survive a police investigation or, at the very least, not be considered important enough to warrant prosecution. On a related note, the reasons behind allocation of police, Crown and prison resources are often related to matters of public policy; just as law acts to affirm and reinforce the values we as a society have determined to be important, so too does it reaffirm a lack of importance. It is my contention, again, that reputation is important and that damage to reputation and the harms attendant upon it are of such importance that they should be matters of public policy, however, to date this is not recognized.³²¹

Criminal defamatory libel provisions have been used to address reputation harm, and have been successful in some cases. A relevant and interesting case prosecuted under this section just concluded in Ottawa. This case dealt with reputation in a few different ways. The facts are as follows: After dining at an Ottawa restaurant, Elayna Katz posted a negative review of the experience on Restaurantthing.com. The restaurant owner retaliated in a number of different ways; first, a number of posts appeared on the site

³²⁰ Although I attempted to find statistics on the frequency and or success rate of prosecutions under these sections, I was unable to do so. Email from Statistics Canada dated 20 November 2012 states in fact that “Statistics Canada does not collect or disseminate information on the conviction of individuals under the libel provisions in the Criminal Code mentioned below”

³²¹ Later in this chapter I will address not only this question of importance but also the role of a new approach in validating that importance even as it recognizes and acts upon it.

sharing Ms. Katz's personal contact information. Restaurant owner Marisol Simoes also rebutted the original review and claimed that Ms. Katz was crazy. A year later, Ms. Katz's employers at the Federal of Canadian Municipalities received an email that purported to be from Ms. Katz that read "I am open to anything -- couples, threesomes and group sex. Am especially into transsexuals and transgenders (being one myself). I am ... a tiger in the bedroom." The same words were used in a profile posted at the same time on an adult site, under men seeking men. Ultimately Ms. Simoes was charged with 2 counts of criminal defamation and found guilty. Despite arguing for a lenient sentence due to the fact that her reputation had already been damaged and that business at her restaurant was suffering because of the publicity, Ms. Simoes was sentenced to 90 days jail time.³²² That is, Ms. Katz's original comment was posted on a restaurant review site and thus at least potentially impacted on the reputation of the restaurant. The retaliation too was reputation focussed, with posts on the same reputation site, emails to her employer which were obviously intended to damage her reputation in that sphere, and the false dating site profile, which again disseminated information intended to damage the reputation of Ms. Katz. Judge Lahaie not only found Ms. Katz guilty, but she likened Ms. Simoes' behaviour to cyberbullying, indicating that the behaviour could have had even more serious consequences, and it was lucky that Ms. Katz was strong enough to withstand the assault on her reputation, and acknowledged that the damage would continue to be perpetuated by records of the incident available through search engines and the like.³²³

The Katz/Simoes case might seem to negate these criticisms – after all, investigation was performed, charges laid, and prosecution initiated and successful – but it need not be understood that way. It is important to take note of the judge's characterization of

³²² Huffington Post. "Marisol Simoes Jailed: Co-Owner of Kinki and Mambo in Ottawa Gets 90 Days for Defamation. <http://www.huffingtonpost.ca/2012/11/16/marisol-simoes-jailed_n_2146205.html>

³²³ Andrew Seymour, "Restaurateur Gets 90 Days in Jail for Criminally Libelling Author of Review (16 Nov 2012) Ottawa Citizen, online: <<http://www.ottawacitizen.com/life/Restaurateur+gets+days+jail+criminally+libelling+author+review/7560754/story.html>>.

the behaviour as “vindictive, vicious and highly personal” as well as her linkage of the behaviour with cyberbullying. While this was a case where the behaviour was egregious enough for a prosecution under the *Criminal Code* to be successful, this does not indicate that every (or any other) reputation damaging behaviour would automatically be dealt with similarly. Indeed, I believe it is unlikely that would be the case.

Thus, while the *Criminal Code* provisions dealing with libel may be applicable to some forms of reputation harm, they are not necessarily the best or most effective response.

Current Legal Approach: Privacy Legislation

If the provisions of the *Criminal Code* aren’t a sufficient way to address reputation, this does not mean that there aren’t other legislative regimes that might be applicable. The Canadian legislation seemingly most relevant to the development, collection and use of reputation information are the public sector *Privacy Act*³²⁴ and private-sector targeted *PIPEDA*.³²⁵

The federal *Privacy and Access to Information*³²⁶ Acts came into force in 1983. The *Privacy Act* applies to personal information that is held by government institutions. Given that the Act defines personal information as explicitly including the views or opinions of an individual about this individual³²⁷, this would very much apply to reputation information. However, the limitation of the scope of the Act means that it could only provide protection in situations where it was a government institution doing the collecting, using or disclosing of the reputation information.³²⁸

³²⁴ R.S.C. 1985, c. P-21 (PA)

³²⁵ *Supra* note 256

³²⁶ R.S.C. 1985, c. A-1 (ATI)

³²⁷ PA s. 3

³²⁸ PA s. 4-8

PIPEDA deals with personal information, which is defined as “information about an identifiable individual.”³²⁹ While reputation certainly fits within this definition of personal information, *PIPEDA* explicitly does not apply to:

- (a) any government institution to which the *Privacy Act* applies;
- (b) any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose; or
- (c) any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose.³³⁰

Obviously, this limits the situations in which *PIPEDA* would be applicable to the reputation information. Reputation information that it does apply to would be regulated with respect to its collection, use and disclosure³³¹ by organizations.³³²

One of the issues that could arise with the application of *PIPEDA* to reputation information is that such information might be considered to be the personal information both of the person who provides the review or assessment as well as s/he who is its subject. It is possible that this nuance might impact or restrict the amount of protection that might be available to an individual. This need not automatically be the case; especially in a formal reputation system, it could be argued that the information is published and as such falls under the Terms of Use of the site hosting it, which would also likely mean that there has been consent (at least implicitly) to the collection, use and disclosure by the person writing the review and participating on the site voluntarily.

³²⁹ *PIPEDA* s. 2(1)

³³⁰ *PIPEDA* S. 4(2)

³³¹ *PIPEDA* sections 3, 5, and 7.

³³² Organization is defined broadly by *PIPEDA* s. 2(1) as including “an association, partnership, person or trade-union”.

It is also noteworthy that both the *PIPEDA* and *Privacy Act* schemes are built upon an ombuds-model. This means that while the Acts do or at least may apply to reputation information, there may be some limits on the protection that they offer in practice, that is, the Acts do regulate the collection, use or disclosure of information and do establish a complaint-based regulatory scheme, however the Privacy Commissioner is given the power to investigate and issue findings, but not to issue enforceable orders.³³³

Thus, the first problem that arises using federal privacy legislation to regulate reputation issues is that there is uncertainty as to the extent the Acts will be considered to apply to reputation information, and even where applicable the extent of actual enforcement (as opposed to ombuds-mediation) is even more limited.

Some have suggested that this kind of data protection approach could be effective in addressing some of the harms inherent in reputation and reputation systems.³³⁴ Certainly there are aspects of *PIPEDA* that would apply. Principles 4 and 5 both have requirements that data be limited to that which is required to fulfill the specified purpose³³⁵ for instance, which could be of assistance both in determining what information is relevant to reputation and in attempting to keep the purposes for which reputation information is consulted to appropriate and relevant ones. Similarly, the rules around the use of information and disclosure of information could apply potentially to the individuals who share information that results in the derivation of reputation, as well as to those individuals or organizations who access reputation information in order to use it in a decision-making process.³³⁶ In order to make *PIPEDA* effective in addressing such issues, organizations and individuals would also be

³³³ In limited circumstances, the Commissioner has the power both to initiate a complaint and to go to Court with such a report to seek enforcement: *PIPEDA* s. 11(2); s. 14. PA s. 29 allows the Commissioner to initiate a complaint under the *Privacy Act*, but the Act does not create the possibility of going to court except in circumstances where access has been denied.

³³⁴ See, for example, Daniel Solove, "The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure" *Duke Law Journal* 53 (2003-4) at 1053.

³³⁵ Principles 4 and 5: *PIPEDA*: <<http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-19.html#docCont>>

³³⁶ *PIPEDA* s. 5-9 <<http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-3.html#docCont>>; Principle 8

required to keep effective records of the collection, use and disclosure of personal information (including reputation information). This would enable access³³⁷ requests to be filled, and accuracy³³⁸ of information to be confirmed or maintained via correction³³⁹ as required by *PIPEDA*. The flaw of data protection laws, however, has always been in their focus on data, rather than individuals.³⁴⁰

Just as in the case of the *Criminal Code*, using these Acts does not appropriately reflect the importance and scope of reputation issues.

Both pieces of legislation are grounded in a data protection approach and as such are focussed primarily on policing data flows rather than on fostering and protecting the rights of those the data pertains to. Additionally, given that *PIPEDA* was passed under federal trade and commerce powers, there can be no question that protection under the scheme would inherently position reputation within an economic rather than a dignity analysis. Overall, then, using these Acts as the avenue through which to address reputation would not be a sufficient response to concerns about reputation.

Current Legal Approach: Private Law

Defamation is not solely the province of criminal law. Indeed, far more common than *Criminal Code* prosecutions are civil suits for the tort of defamation. A civil suit is, essentially, a legal action seeking redress, but one that does not involve criminal liability. Rather, it is a private legal action, based in common law.

Although based in common law, the tort of defamation and its attendant defences are very similar to those already examined in the *Criminal Code*; indeed, the *Criminal Code*

³³⁷ *PIPEDA* s. 8 <<http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-3.html#docCont>>; Principle 9

³³⁸ *PIPEDA* Schedule 1, Principle 6

³³⁹ *PIPEDA* Schedule 1, Principle 4.9.5

³⁴⁰ Jennifer Barrigar, *Is You Is Or Is You Aint: Making PIPEDA's Rights Language Meaningful by Re-Viewing Social Value*, University of Ottawa, 2006) [unpublished]

in this case functions essentially as a codification of the common law, with the attendant force of the justice system behind it.

At its most basic then, defamation is the act of publishing information that is damaging to a person's reputation.³⁴¹ As such, the whole field of defamation is grounded in recognition of the importance of reputation.

Brown states the basics of the tort as follows:

In order to recover in an action for defamation, the plaintiff must show that:

- a) the words about which the plaintiff complains are defamatory;
- b) they referred to the plaintiff; and
- c) they were published to a third person.

If the words are not actionable per se, the plaintiff must also show that he or she suffered special damages.³⁴²

Defamation is (primarily) a strict liability tort, meaning that a person will be held liable for a defamatory publication regardless of: intent to make a statement at all³⁴³; intent to defame³⁴⁴; whether the defendant intended or believed the information to be false³⁴⁵; absent direct referral to the plaintiff³⁴⁶; and even absent any damage being caused.³⁴⁷

Although the language of "publication" might suggest some concerns with dissemination over the internet, just as with the *Criminal Code* provision, this is not the

³⁴¹ Raymond E. Brown, *Defamation Law: A Primer* (Toronto: Carswell, 2003) 4

³⁴² *Ibid.*

³⁴³ *Burton v. Crowell Publishing Co.*, 82 F.2d 154 (2d Cir. 1936).

³⁴⁴ *Cassidy v. Daily Mirror Newspapers*, [1929] 2 K.B. 331 (C.A.)

³⁴⁵ *Allan v. Bushnell T.V. Co.*, [1969] 2 R. 6 (C.A.)

³⁴⁶ *E. Hulton & Co. v. Jones*, [1910] A.C. 20 (H.L.)

³⁴⁷ *McRae v. South Australian Telecasters Ltd.* (1976), 14 S.A.S.R. 162 (S.C.)

case. Publication means “the transmission of a defamatory idea to a third person.” Where the publication takes place by virtue of general dissemination in a public space (such as a supermarket³⁴⁸) “publication” can be crystallized by showing that the words were spoken in a loud enough voice so that the persons nearby could have heard and understood the defamatory words. The act of putting such comments in an area of the internet that is publicly accessible would likely be treated similarly, with evidence that the page or site has been visited being considered sufficient to indicate that persons could have heard (seen) and understood the defamatory words.

The requirement of a deliberate act or active participation has been developing in Canadian law and was emphasized in *Crookes*.³⁴⁹

The defence of innocent dissemination was created in *Vizetelly v. Mudie's Select Library Ltd.*, and fleshed out in *Crookes*, currently the leading Canadian case on internet defamation.

In *Vizetelly*, the court framed the requirements for establishing innocent dissemination using three stages:

1. the defendant did not know that the publication complained of contained a libel;
2. the defendant had no grounds to suppose that it was likely to contain defamatory matter; and
3. The absence of knowledge was not due to any negligence on the defendant's part.

The *Vizetelly* test does not require certainty of the existence of defamation on the part of the site, only negligence in not addressing it. Although originally developed in order to excuse ISPs from being found liable for content they passively hosted, it is possible

³⁴⁸ *Food Lion v. Melton*, 250 Va. 144, 458 S.E. 2d 580 (1995)

³⁴⁹ *Crookes v. Wikimedia Foundation Inc.*, 2008 BCSC 1424 (CanLII), <<http://canlii.ca/t/21b1z>> retrieved on 2012-12-15 201.

that this defence could be invoked in relation to defamation. It is unlikely, however, that it could be successfully applied to a systematized reputation situation.

This failure to apply comes about because the nature of such a system could, and indeed likely should, lead to the conclusion that the site had grounds to *suppose* that the reputation system *likely* contained defamatory matter. Where a site's business model relies on the posting of both negative and positive comments to garner trust amongst users, it is evident that even (or perhaps especially) users who have a negative experience will leave feedback. Design that relies on feedback information which will include negative feedback should lead any reasonable site administrator to suppose that the feedback system may, or even most likely will, contain defamatory material. Any willful blindness to the likely existence of defamation would fall under negligence in the third stage of the *Vizetelly* test.

Further support for the argument that innocent dissemination would not apply to reputation systems can be found in the recent Supreme Court of Canada decision in *Crookes*, where the novel methods of information sharing on the internet spurred the court to adopt a more contextual approach to innocent dissemination. The court in *Crookes* uses "comparator groups" to assess the nature of an online business' role in the dissemination of information. That is, faced with a novel method of information dissemination (such as reputation systems); the *Crookes* approach compares the method to recognized categories, such as publishers and book retailers. The result is the ability to fit novel methods of dissemination into established categories such as carriers, distributors and publishers. These categories are again consistent with an approach that eschews a finding of defamation for carriers or distributors rather than those with any responsibility for the actual content. It is important to note, however, that any business model that relies on reputation or other feedback, in order to facilitate user trust and comfort with the site, is not one that is consonant with distribution; this is an active relationship rather than a mere passive role.

The requirements to bring an action for defamation are fairly simple; the complainant must have a reputation and must have been, or believe herself to have been, defamed.³⁵⁰ As for the defendant, unlike the *Criminal Code* provision which did not specify any conditions, under the tort of defamation the defendant must be a legally recognized person and be responsible for the publication of the allegedly defamatory statement. Again, this is a situation where the various layers of reputation and reputation systems may result in a poor fit with existing legal remedies. Online reputation, especially when looking at a formalized reputation system, may lack an easily identifiable individual (due to anonymity, pseudonymity, etc) and an aggregate reputation may not be promulgated by a legally recognized person. Indeed, while there exists a legal fiction that corporations and other formal entities may be recognized as legal persons, case law shows that complainants have been unsuccessful at holding an unincorporated association responsible at law for defamation due to the lack of a unified/recognized legal “self”.³⁵¹ Thus, the aggregate reputation and the site which publishes it may be shielded from civil action by virtue of loose or no formal associations.

In reviewing case law on defamation, it is interesting to note the way(s) in which reputation is parsed by experts and judges. Lord Denning pondered the question extensively, writing:

A man’s “character”, it is sometimes said, is what he in fact is, whereas his “reputation” is what other people think he is. If this be the sense in which you are using the words, then a libel action is concerned only with a man’s reputation, that is, with what people think of him; and it is for damage to his reputation, that

³⁵⁰Raymond E. Brown, *Defamation Law: A Primer* (Toronto: Carswell, 2003) at 79. Interestingly, Brown insists that the complainant must not only have a reputation, but must have a reputation that is capable of being defamed. It seems to be, however, that this is too subjective – surely any reputation, no matter how low it seems, may be harmed further. Indeed, if a potential complainant had lacked any reputation prior to the harm, s/he would still, it seems to me, have standing to bring suit because in the act of harming, some reputation would be established.

³⁵¹ *Ibid.*

is, to his esteem in the eyes of others, that he can sue, and not for damage to his own personality or disposition.

The word “character” is often used, and quite properly used, in the same sense as the word reputation. Thus, when I say of a man that he has always borne a good character, I mean that he has always been thought well of by others; and when I want to know what is character is, I write, not to him, but to others, who know something about him. In short, his character is the esteem in which he is held by others who know him and are in a position to judge his worth. A man can sue for damage to his character in this sense, even though he is little known to the outside world....But a man’s character, so understood, may become known to others beyond his immediate circle. In so far as the estimate spreads outwards from those who know him and circulates among people generally in an increasing range, it becomes his reputation, which is entitled to the protection of the law just as much as his character. But here I speak only of a reputation which is built upon the estimate of those who know him. No other reputation is of any worth. The law can take no notice of a reputation which has no foundation except the gossip and rumour of busybodies who do not know the man. Test it this way. Suppose an honourable man becomes the victim of groundless rumors. He should be entitled to damages without having this wounding gossip dragged up against him. He can call people who know him to give evidence of his good character.³⁵²

Brown boils this down to:

“Reputation” is the estimation in which a person stands in the opinion of others. It reflects his or her moral or social worth in the community. It differs from “character” which defines a person by the traits he or she actually possesses. Character identifies the person as he or she really is; reputation is what he or she appears to be to others.³⁵³

It should be noted that although Brown speaks of the reputation of the person, it has been established that companies, organizations and unions have the ability to bring suit for defamation. This is of interest because it makes clear that defamation is not about “hurt feelings” since these are not persons and do not have feelings; rather, extending

³⁵² *Plato Films Ltd. V. Speidel*, [1961] A.C. 1090 at 1138 (H.L.)

³⁵³ Raymond Brown, *Defamation Law: A Primer* at 5

the range of potential complainants of defamation makes it evident that this is about reputation as an external thing, rather than about internal harm.³⁵⁴

These distinctions are of particular interest when we examine the internet, given the way reputation has come to stand in for identification in some arenas. That is, no longer are individuals required to identify themselves, rather they are asked to point to some reputational ranking. Reputation thus presumptively authenticates a person and may even take the place of identity.³⁵⁵

Instead of distinguishing between internally (character) and externally (reputation) generated selves, the external comes to stand in for the entire person. This is not to suggest that the reputation is the person; as has been discussed, reputation is externally derived and as such is separate from the individual even as it becomes used to validate or authenticate them. Among other things, this means that one cannot claim defamation merely because the reputation accorded you is undeserved. Only when the reputation that pre-exists is damaged by the defamatory actions of another can such a claim be made. In determining whether such damage has been suffered, the standard used to assess whether reputation has been lowered is an objective, not subjective one. In Canadian jurisprudence, the test is that of the objective “reasonable person”.³⁵⁶

Of course, tort law has always been intended as a flexible response, able to take account of changing cultures and standards. This is evident in the test itself; just as the earlier discussion of reputation showed it to be grounded in community standards, so too was the early legal language inherently moralistic, focussing on “shameful” behaviour. This very flexibility, however, is one of the problems attendant on attempting to use the tort

³⁵⁴ Elad Peled, "Should States Have a Legal Right to Reputation? Applying the Rationales of Defamation Law to the International Arena" *Brooklyn Journal of International Law* 35:1 (2010) at 120

³⁵⁵ Given the embedding of the transoptic perspective and the attendant risk of mainstream assumptions negatively impacting on an individual, this also creates a risk of becoming a kind of social sorting.

³⁵⁶ Kate Sutherland, "The Impact of the Tort of Defamation on Public Discourse About Racism" in Rakhi Ruparelia, Sandra Rogers & Louise Belanger-Hardy eds., *Critical Torts* (2009) 135 at 137.

of defamation to address reputation violations. It is a problem (and an evolving one) due to the increasingly fragmented nature of the publics within which we interact. This is because the defamation that is claimed must be recognized within the social sphere in which it occurs (otherwise there is not damage to reputation), but also must be something that is recognized in the judicial assessment of the “reasonable person”. Comments or assessments that could be unexceptional inside a community may appear unreasonable to a “reasonable person” operating from more mainstream standards, and vice versa. Remembering too that it is not just the actual text of a statement, but the inferences that may be drawn from it, to which defamation applies, the need to fully understand the social context in which the incident arises becomes even more imperative. How can the reasonableness of an inference be assessed by those working within a different frame of reference than the community who received the comment and/or drew inferences?³⁵⁷ Perhaps related to the above distinction between “character” and “reputation”, it should be noted that:

Mere insult or vulgar abuse, however, is not defamatory. The words must be more than unpleasant and disagreeable. Language which is simply crude, offensive and in bad taste, or which affronts only a person’s dignity, but does not otherwise lower him or her in the esteem of others, is generally not actionable. Some allowance must be made for name calling particularly in the context of angry confrontations where parties exchange words of insult and abuse which are understood as such and nothing more. A defendant is not to be held accountable in defamation merely because he or she exhibits bad manners and engages in minor discourtesies.³⁵⁸

One of the principles of defamation and interpretation is that the whole context of a statement counts, but denuded of context as the internet may be argued to be, is this possible? How can we determine which statements are sheer anger or abuse and which are inherently defamatory?

³⁵⁷ Raymond Brown, *Defamation Law: A Primer* at 26

³⁵⁸ *Ibid.*

Returning to the discussion(s) in chapter 3, it is evident that online spaces don't just facilitate the dissemination of information; they also facilitate the development of a variety of very disparate publics, each with their own system of norms and values. Social interactions online, then, are not denuded of context; as with any space, they are filled with multiple contexts, created, negotiated and re-created by the participants. For a reasonable person to make a reasonable assessment of defamation, the full context within which a comment occurs must be factored in. When it is not, then just as mainstream norms influenced the original comment so too may they influence the assessment of that comment, in the process skewing justice.

Another interesting aspect of the necessity of understanding and incorporating the entire context is Strahilevitz's suggestion that people have a tendency to overestimate their own centrality in networks, and thus that they will accordingly overestimate what people would find worth discussing.³⁵⁹ This may cause problems of its own if the assessment of the "reasonable person" weighs the violation against the potential for damage and concludes that little or no protection is required because the violation is proportionally insignificant.

Defences available to an action for defamation are:

- a) the words are true (justification);
- b) the plaintiff consented to the defamatory publication;
- c) the words were spoken on an occasion of absolute privilege;
- d) the words were spoken on an occasion of qualified privilege and the plaintiff is unable to show that the defendant was malicious;
- e) the words were contained in a privileged report of judicial or legislative proceedings or in other reports or documents protected by statute; and
- f) the words are fair comment made honestly and in good faith on a matter of public interest.³⁶⁰

³⁵⁹ Lior Jacob Strahilevitz, "A Social Networks Theory of Privacy" (2005) 72 *University of Chicago Law Review* at 985

³⁶⁰ Raymond Brown, *Defamation Law: A Primer* at 22

One of the defences to a claim of defamation is that the plaintiff consented to the defamatory publication. This could present some problems with invoking defamation in the context of reputation systems in online environments. It is that presumptive publicness discussed earlier; if that is the starting point, it might be argued that any individual who participates on eBay, Slashdot, etc. is aware of the reputational feature of the site and thus their participation counts as implied consent to the publication. I do not agree. A more nuanced understanding of reputation as social artefact indicates that while consent may have been given for those on the site to watch my behaviour and report on transactions and interactions, my consent extends only that far. Just because I consented to and participated in reputation production in one context does not equate to consent for those interactions to be broadcast outside of that situation, especially not in different contexts or with different inferences attached to them. Remembering that the consent defence under the *Criminal Code* was very narrowly defined to cover only specific consents, it is uncertain how generously consent would or could be interpreted outside the criminal law. Certainly, Brown suggests that the interpretation of consent is very specific³⁶¹. Given this, it seems at least arguable that the argument that mere participation on a site would not be sufficient to indicate implied consent to the publication of defamatory statements would be consistent with existing law. While there is jurisprudence that shows that knowledge that a publication may be defamatory will be sufficient to ground a defence of consent,³⁶² I do not believe that a request for reasons why one was denied a job is analogous to the knowledge that one may be subject to review. In the one case, the plaintiff was known to have expected the reasons to be negative and ill-founded, where in the latter case it is surely reasonable for an individual who conforms to the stated site rules to believe that a review will appropriately reflect that.

³⁶¹ Raymond Brown, *The Law of Defamation in Canada* at 394

³⁶² *Hanley v Pisces Productions Inc.*, [1981] 1 W.W.R. 369 (B.C.S.C.)

Issues of qualified and absolute privilege are also unlikely to be effective defences in this arena, although participation in a site that uses a reputation or feedback system may imply some form of duty to participate, it is not the kind of formal duty (with attendant penalties for failure to do so) contemplated by these defences.³⁶³ Similarly, given that these are individual assessments, there is little or no likelihood that the words will emanate from published reports or that they would be protected by statute.

The defence of “fair comment” has recently undergone some changes thanks to the 2008 Supreme Court of Canada decision in *WIC Radio*.³⁶⁴ In that decision, a previously dissenting view was revisited and adopted by the Court. As a result, the test set out by Justice Dickson in his dissent in *Cherneskey v. Armadale Publishers Ltd.*³⁶⁵ has now become the standard by which fair comment will be assessed. That test is:

- a) the comment must be on a matter of public interest;
- b) the comment must be based on fact;
- c) the comment, though it may include inferences must be recognizable as a comment;
- d) the comment must satisfy the objective test: could any person honestly express that opinion on the proved facts?
- e) even where the comment meets all of the previous requirements, the defence may still fail if the plaintiff is able to show that the defendant was acting with malice.³⁶⁶

With this change comes another area where the tort of defamation may not map effectively on to reputational damage; that of reputation systems. It is questionable that the understanding of “public interest” is broad enough to encompass either an individual’s performance on a site or community, or the assessment made thereof. Interestingly, although the decision parses the defence of fair comment, it never

³⁶³ Kate Sutherland, “The Impact of the Tort of Defamation on Public Discourse About Racism” *Critical Torts*, edited by Rakhi Ruparelia, Sandra Rogers and Louise Belanger-Hardy (2009) 135 at 145.

³⁶⁴ *WIC Radio Ltd. v Simpson* [2008] 2 S.C.R. 420

³⁶⁵ [1979] 1 S.C.R. 1067

³⁶⁶ *WIC Radio*, paraphrased from Sutherland, at 144.

directly addresses the determination of what is in the public interest. Reference is made to public controversy and discussion, but no threshold for the underlying “interest” is set. As this project has sought to establish, when it comes to reputation, the question is not one of public but of multiple co-extensive publics. My concern is that this same multiplicity of publics may be presumed to undermine a recognizable “public interest” by making the issue appear to be of special rather than public interest.

Additionally, the dual levels operating in the assessment process may create difficulties in determining which “interests” should be assessed; the panoptic effect intended by the designers of a formal reputation system? Or the synoptically-derived standards developed within and shared by the users and accordingly imported into the reputation mechanism. What about identity performances within an informal reputation arena; how can standards, performances, inferences and assessments be isolated and identified, let alone addressed through this defence?

Similarly, which facts need be proved? Those related to the site design’s putative function? Or those related to the community standards? Whose community? Can socially derived, created and re-created standards be isolated and identified sufficiently for the purposes of a court of law?

In relation to the efficacy of the tort of defamation in dealing with reputational injury, it should also be noted that damages for defamation may be mitigated by evidence that the plaintiff already had a “bad reputation.”³⁶⁷ Many/most reputation systems are cumulative, making it virtually (no pun intended) impossible to isolate the impact of a particular piece of feedback in a sea of related feedback. Thus, an individual’s libel may be integrated by the algorithm, impacting s/he who is reviewed even as the reviewer is shielded from responsibility.

³⁶⁷ Raymond Brown, *The Law of Defamation in Canada* at 227

As previously discussed, the nature of reputation, as well as the insertion of mainstream synoptically derived norms into formal reputation systems (and their impact on informal reputation assessments), has the effect of privileging those who conform to mainstream expectations or standards. This is another aspect that makes the tort of defamation less than ideal as a response to reputational harm because it may obscure the court's ability to understand what is at issue. That is, while mainstream norms or expectations may have particularly negative implications for Others, where those norms are shared at the judicial level the comments may be protected by a presumption of 'trueness' rather than understood within the particular social interaction as extraneous, and thus ultimately defamatory.

Ultimately, then, the tort system, while it may provide redress for some reputational harms, is clearly not the most effective or desirable avenue. Litigation is expensive and slow with unpredictable outcomes, and the system is very much a one-on-one affair and thus has no larger social transformative or deterrent effect.

Aspirational Approach: Human Rights Law

Having canvassed the legal approaches that are currently in use and found them lacking as an appropriate response to the full complexity of reputation, there is one final existing approach that might potentially be invoked, though it is not currently understood as applicable to reputation specifically. I speak, of course, of looking at reputation within a human rights framework.

Article 12 of the *Universal Declaration of Human Rights* states that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."³⁶⁸ Similarly, the *International Covenant on Civil and Political Rights*, Article 17, states that "[n]o one shall be subjected

³⁶⁸ UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III), available at: <http://www.unhcr.org/refworld/docid/3ae6b3712c.html> [accessed 15 December 2012]

to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.”³⁶⁹

Reputation is not contained in the Canadian *Charter of Rights and Freedoms*, nor is it named in the federal or most provincial human rights legislation³⁷⁰. In Canada, legislation, especially human rights legislation, is considered a “living tree”³⁷¹, meant to grow and change with society. It is incontrovertible that there are contained within this legislation bases of discrimination that were not contemplated at the time of the original drafting. Thus, the mere fact that reputation is not currently contained within Canadian human rights legislation is not necessarily a barrier to it being addressed via a human rights framework

Section 2 of the *Canadian Human Rights Act* sets out the purpose of the legislation as follows:

The purpose of this Act is to extend the laws in Canada to give effect, within the purview of matters coming within the legislative authority of Parliament, to the principle that all individuals should have an opportunity equal with other individuals to make for themselves the lives that they are able and wish to have and to have their needs accommodated, consistent with their duties and obligations as members of society, without being hindered in or prevented from doing so by discriminatory practices based on race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital status, family status, disability or conviction for an offence for which a pardon has been granted.³⁷²

³⁶⁹ UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, available at:

<http://www.unhcr.org/refworld/docid/3ae6b3aao.html> [accessed 15 December 2012] p. 171,

³⁷⁰ Only Quebec includes reputation – s. 4 of the Quebec *Charter of Human Rights and Freedoms* guarantees the right to “the safeguard of his dignity, honour and reputation”. R.S.Q., c. C-12.

³⁷¹ *Edwards v. Canada (Attorney General)* [1930] A.C. 124, later invoked specifically with reference to the Charter in *Reference re Section 94(2) of the Motor Vehicle Act*, [1985] 2 S.C.R. 486

³⁷² *Canadian Human Rights Act* (R.S., 1985, c. H-6), online: <<http://laws.justice.gc.ca/PDF/Statute/H/H-6.pdf>> (Accessed 9 August 2010)

In 2000, a review of the *Canadian Human Rights Act* was conducted by a Commission headed by former Supreme Court of Canada Justice La Forest. In chapter 3 of that report, examining the history and purpose of the Act, he traces the evolution of its interpretation from formalistic intentional discrimination, through to the recognition of adverse effects discrimination and into the eventual understanding of systemic discrimination. Speaking of systemic discrimination, the report states:

Looking at discrimination in this way recognizes that human activities, such as employment and the provision of services, proceed on the basis of assumptions and value judgements about the capacities and needs of individuals. These assumptions often reflect ideas about the place in society of certain individuals because of their personal characteristics. This in turn may be reflected in the way the workplace is ordered, in the terms and conditions of employment, and in decisions about who should be hired and promoted. While some of these assumptions may be accurate, others are harmful in that they create barriers to the full participation of individuals in the workplace or in access to services.³⁷³

Contemplating these words, it seems evident that reputation could be addressed within such a framework. Reputation, as has been shown, is itself the product of assumptions and value judgements about the worth of an individual. Further, analysis of the dual levels of assessment taking place within formal reputation systems demonstrated how (mainstream) assumptions and stereotypes may be inserted into the most objective-seeming review; this too accords with the recognition that assumptions may be harmful. Finally, exploring the way(s) in which access to knowledge, information, employment or services may be limited or barred as a result of reputation, again makes evident the parallels, since reputation too may create barriers to the full participation of individuals in the workplace or in access to services.

It should be noted, as well, that while reputation itself is not explicitly contained in the *Canada Human Rights Act*, the recognized bases of discrimination in that Act -race,

³⁷³ LaForest & et al., "Promoting Equality: A New Vision" Report of the Canadian Human Rights Act Review Panel(2000).

national or ethnic origin, colour, religion, age, sex, sexual orientation, marital status, family status, disability or conviction for an offence for which a pardon has been granted – are all factors that may impact on reputation assessments themselves. Arguably, this is further evidence that reputation is not just analogous to the currently recognized bases of discrimination in the Act, but indeed is to some extent already incorporated into their analysis.

Opposition to this approach may raise the issue of immutability, that is, that the characteristics generally protected under human rights legislation are immutable characteristics whereas reputation is not. There can be multiple responses to this.

It is worth noting that not all characteristics protected under such rubrics are in fact immutable. Issues of marital status, criminal convictions, and even family status are certainly issues that support recognition of human rights protections as extending beyond immutable characteristics.

On a related note, it is also useful to consider Kenji Yoshino's arguments around what he terms "the new civil rights". With an argument located in questions of sexual orientation, Yoshino distinguishes the traditional or classic model of human rights protections, which are based on an immutable characteristic model. He does so distinguishing between different types of visibilities when it comes to discrimination; corporeal visibility and social visibility. He defines them as:

...by corporeal visibility, I mean the perceptibility of traits such as skin color that manifest themselves on the physical body in a relatively permanent and recognizable way. Social visibility, on the other hand, designates the perceptibility of nonphysical traits.³⁷⁴

³⁷⁴ Kenji Yoshino, "Assimilationist Bias in Equal Protection: The Visibility Presumption and the Case of 'Don't Ask, Don't Tell'" (1998-99) 108 *Yale Law Journal* 485 at 497

Thus, in social visibility, it is not a characteristic discriminated against, but rather the activity of expressing or performing. While simply choosing not to (actively) disclose difference online in order to avoid Otherness may seem to be an option, it is not without its own problems. As Yoshino notes:

The fact that the expression of a trait is discretionary does not mean that its possessor holds that discretion; to the contrary, social actors can often wrest that discretion away from the possessor of the trait. By doing so, such actors can control the possessor's identity in a way that could not be applied to those who bear traits whose expression is not discretionary.³⁷⁵

In the case of (re)presentations of identity within the Internet, the identity of one who possesses (or has ascribed to her) an Other trait may not always be controlled by the social actor themselves. As discussed earlier, direct self-identification is not the only means by which an Other body is ascribed to a participant within the Internet. Thus, it is not only acts of direct self-identification which must be guarded against, but rather a constant policing of the content of one's (re)presentations to screen out "deviant" thoughts or ideas which may attract scrutiny. Jenny Jones has noted, "having to remain vigilant against revealing negative self-features does not permit the person to forget about or de-emphasize this aspect of identity – quite the contrary."³⁷⁶ The choice to remain silent enacts a constant panoptic consciousness of scrutiny, and to some degree wrests control of identity from the individual. Thus, both forced disclosure and forced repression are at issue for anyone who strays from the presumptive norm online. That is, by creating a situation where a particular identity is presumed (forced repression) unless it is explicitly claimed either through self-identification or even through

³⁷⁵ Kenji Yoshino, "Assimilationist Bias in Equal Protection: The Visibility Presumption and the Case of 'Don't Ask, Don't Tell'" (1998-99) 108 *Yale Law Journal* 485 at 536.

³⁷⁶ Jenny Jones, "Reproduction and the Creation of the Digital Image" (1999) 9 *N. Paradoxa: international feminist art journal* at 683

commentary on issues which lead to the ascription of identity (forced disclosure), constant normative pressure is applied to the individual not to “become” Other.³⁷⁷

Nor is the harm done by the choice to remain silent only that of fear of revelation (although the impact of such fear should not be underestimated). As Yoshino notes, “expression is not just an effect of an underlying identity, but potentially a cause of it as well. Thus, when that expression is burdened, the burden is not only an epistemic harm but also an ontic one.”³⁷⁸ Thus, not just consequences, but identity itself may be implicated by such a decision.

The human rights process contains within it the flexibility to address issues of anonymity, by allowing pseudonyms or even by allowing the Commission to initiate a complaint themselves. Section 13 of the Act, governing hate speech, is already recognized as applying to the Internet as well as to other means of communication, and thus this is a law of general application that is demonstrably able to address online issues and practices. Finally, as a publicly funded tribunal, the process alleviates the expense and the antagonism of civil actions.

Thus, although there are a number of ways in which human rights protections may be extended to protect online reputation, there are still a number of factors that limit the effectiveness of these kinds of responses.

Despite the fact that human rights legislation addresses discrimination based on protected grounds, and reputation is intimately involved with those same protected grounds, the focus on discrimination would have the effect of limiting the protection of reputation rather than of increasing it. That is, having established that reputation is

³⁷⁷ This notion that claiming our non-neutral identities creates social prejudice takes us back to Yoshino’s notions about identifiability and, at least arguably, may provide the ground from which to re-view anti-discrimination policies and practices.

³⁷⁸ Kenji Yoshino, “Assimilationist Bias in Equal Protection: The Visibility Presumption and the Case of ‘Don’t Ask, Don’t Tell’” (1998-99) 108 *Yale Law Journal* 485 at 530.

multi-faceted, deeply nuanced, and socially and culturally embedded in most, if not all, interactions, a regulatory scheme intended to address reputation should protect all reputation-based injuries.

Human rights protection, although intended as transformative, effectively redresses discrimination on protected grounds. Section 5 of the *Canadian Human Rights Act* states that:

5. It is a discriminatory practice in the provision of goods, services, facilities or accommodation customarily available to the general public (*a*) to deny, or to deny access to, any such good, service, facility or accommodation to any individual, or
- (*b*) to differentiate adversely in relation to any individual, on a prohibited ground of discrimination.

While I have shown that reputation may well be influenced by many of the protected grounds set out in the Act (race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital status, family status, disability and conviction for an offence for which a pardon has been granted or in respect of which a record suspension has been ordered.³⁷⁹), this is not always the case; reputation may be grounded on assessments of performance that do not rely upon these grounds yet still result in limitation of access, as in the situation where a negative eBay score prevents an individual from participating in future transactions. Thus, for reputation to be effectively protected, the protection must reside not in a denial predicated upon reputation, but rather relate to reputation directly.

It might be pointed out that s. 13 of the *Canadian Human Rights Act* protects against hate speech, regardless of discrimination upon those grounds and that it should be possible to amend human rights legislation to protect reputation in a similar fashion. It is important to note, however, that the hate speech provisions of the Act do speak to the

³⁷⁹ *Canadian Human Rights Act* s. 3(a)

protected grounds by applying to communication that exposes “a person or persons to hatred or contempt by reason of the fact that that person or those persons are identifiable on the basis of a prohibited ground of discrimination.”³⁸⁰ Thus, there is still an action at issue; here, the act of communication that exposes persons to hatred or contempt.³⁸¹

Finally, as I have shown in the previous chapters, reputation is a complex issue, one that is integrally related to an individual’s identity and social relationships. The ways in which “people encounter, use, and experience information and how those practices inform the development of culture and identity”³⁸² cannot be easily (or at all) reduced to a simple set of statements, even one as broad as the language of s. 5’s “goods, services, facilities or accommodation customarily available to the general public.” Reputation impacts on the way(s) in which we understand our society and each other as well as the way(s) in which we interact; these are things that transcend the tangible, and certainly things that extend beyond simply the provision of goods, services, facilities or accommodation.

Conclusion

A review of the existing legal responses that might be employed to address issues of reputation in online spaces demonstrates, then, that current methods are simply not sufficient to the full complexity of the issue.

Criminal law deals with many aspects of reputation, but was shown to be not the most effective means of addressing the issue because it denied complainants agency and was overly narrowly focussed

³⁸⁰ *Canadian Human Rights Act* s. 13(1)

³⁸¹ It should also be noted that despite the Federal Court decision on 3 October 2012 in *Warman v. Lemire* that the Human Rights Tribunal had erred in refusing to apply s. 13(1). Bill C-304, which would eliminate s. 13 from the CHRA, has passed the House of Commons and is currently at first reading in the Senate. Thus, arguments based on s. 13 may not be particularly relevant or useful in the near future.

³⁸² Julie E. Cohen *Configuring the Networked Self* at 5

Private law addresses many of the same aspects as criminal law but without government intervention. Sadly, the one to one feature of private law is also its weakness because private systems necessarily eschew any possibility of social transformation.

Current privacy legislation, both public and private sector, coming from a data protection standpoint, also falls short in dealing with reputation, focussing on data to the detriment of understanding impacts.

Finally, human rights legislation (which does not currently address reputation *per se* but which I have shown could potentially do so) does seem best placed to address the issue but still is too limited to address the full complexity of reputation and its social and cultural impact(s).

Having established the complexity of reputation and the increasing way(s) it is impacting, and potentially impacting, individuals in Part I, in Part II I am moving on to the question of how and whether the area could or should best be regulated.

In this chapter I reviewed the existing legal approaches that are or could be applied to reputation in order to assess their effectiveness in addressing the situation. As has been seen, there are aspects of each approach that seem applicable, but ultimately none of the approaches is capable of addressing (and redressing) the intricacies and ramifications of reputation.

CHAPTER 6: Stupid User: Re-Viewing and Re-Placing Responsibility

Having grounded the idea of reputation as social artefact and shown the ways reputation is increasingly being used and misused in Part I, Part II is now engaged in re-viewing regulation of the area. The focus shifts now to look at the question of how such complex social systems can or should be regulated.

In the previous chapter, existing legal approaches were assessed to determine their efficacy in addressing reputation in all its complexity. The determination at the end of that process was that while each of the existing schemes had some aspects that addressed reputation, none of them was sufficient to deal appropriately with the entirety of the issue.

Although existing legal channels have been exhausted, this does not mean that there are no forces acting to shape social and reputational interactions. Accordingly, my examination turns now to look at the variety of other avenues through which some regulatory force may be being exerted.

In this chapter, I will set out the underlying expectations that inform public and governance attitudes towards reputation. As such, this chapter examines and explores the process of “responsibilization”, examining the shift from a society under government control to one where risk management and self-protection have become increasingly the province of the individual, at least in public perception.

Introducing the Stupid User

A. After purchasing an electronic device with data capture capabilities, the consumer returns it to the store. Weeks later, s/he is horrified to discover that a stranger purchased the computer from the store and found the consumer's

personal information still on the hard drive.³⁸³ Surely only a “stupid user” would fail to delete their personal information before returning the device, right?

B. A Quebec woman is off work on disability due to depression. During this time, after consultation with her psychiatrist, she engages in a number of activities intended to raise her spirits, including a visit to a Chippendale’s review; a birthday party; and a tropical beach vacation. Suddenly, her benefits are terminated and she is told by her insurance company that they had viewed photos on her Facebook page that showed her looking happy and therefore they considered her not to be depressed and thus able to return to work.³⁸⁴ I mean, really – if you’re going to post all these happy pictures, surely you were asking for such a result? Stupid not to protect yourself, isn’t it?

C. An RCMP Corporal is suspended from the force and subject to an investigation into sexually explicit photographs in which s/he allegedly appears are posted to a sexual fetish website.³⁸⁵ Surely anyone who is in a position of responsibility should know better than to take such photos, let alone make them public. How can we trust someone who makes such a stupid error to do their job and protect us?

In media reports, in discussions, at conferences, there are discussions about personal information and reputation in online spaces, the spectre of the “stupid user” is raised. Posting of “risky” information, “failure” to use the privacy tools built into online spaces, “failure” to appropriately understand the permanence of online activities and govern

³⁸³ Office of the Privacy Commissioner of Canada “Chapter 3: Destruction of Data in the Digital Age” Annual Report to Parliament 2010: Report on Personal Information Protection and Electronic Documents Act online: <http://www.priv.gc.ca/information/ar/201011/2010_PIPEDA_e.asp#sect5>. See also Audit Report of the Privacy Commissioner of Canada: Staples Business Depot: Final Report>. 2011 online at <http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_staples_2011_e.asp>.

³⁸⁴ <http://news.cnet.com/8301-17852_3-10404633-71.html>

³⁸⁵ <<http://www.cbc.ca/news/canada/british-columbia/story/2012/07/05/bc-rcmp-sex-photos.html?cmp=rss>>

ones activities and information about oneself³⁸⁶ accordingly; these actions (or lack thereof) are attributed to the mythical “stupid user”. Even if you’ve not heard the phrase, you’ve probably encountered the idea. It’s a pretty common occurrence these days; the question of privacy and Facebook comes up and everyone is an expert. The air around you is suddenly filled with voices, everyone trying to explain that once you put information on Facebook or really anywhere at all, to talk about privacy is ridiculous. That ship has sailed, someone will explain patiently, information online is information you’ve released into the wild. You have no privacy; you have no control over the information at all!

Presumptive Publicness and the Stupid User

This phenomenon isn’t restricted to expressions of advice or concern. As shown in the examples above, the idea that information once recorded (especially online) is presumptively public becomes the foundation for responses to many situations; responses that focus on the actions, errors and most of all the responsibility of the individual(s) in the situation rather than the larger issues that may be in play.

A: STAPLES

In 2011, the Privacy Commissioner of Canada released the results of an audit into Staples Business Centre³⁸⁷ as well as speaking about those audit results in her Annual Report to Parliament.³⁸⁸ Although the audit looked at a number of practices of Staples’ overall, the Commissioner’s comments in the Annual Report focussed on the issue of personal data contained on storage devices that are returned to Staples and ultimately resold.

³⁸⁶ One of the reasons that this project speaks of reputation and activities generally rather than focussing solely on the online component is the recognition that information about one’s offline activities (including photos, blog posts and other tales) as well as online activities may become part of the public record through our own actions or those of others.

³⁸⁷ <http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_staples_2011_e.cfm>

³⁸⁸ <http://www.priv.gc.ca/information/ar/201011/2010_PIPEDA_e.cfm>

Recognizing that *PIPEDA* places an obligation on Staples to implement technical, physical and organizational safeguards to protect customers' personal information under their control, the Privacy Commissioner ultimately found that although Staples had instituted procedures and safeguards to address the issue, those procedures were not always followed, nor were they necessarily sufficient to protect the personal information. Accordingly, the Privacy Commissioner concluded that:

Ineffective processes and procedures surrounding data storage devices were the subject of two previous complaints filed against Staples with this Office. These complaints involved privacy breaches, where personal information on data storage devices had not been adequately erased prior to being resold, resulting in the improper disclosure of personal information to other customers. Staples committed to taking corrective action, including implementing a full "wipe and restore" procedure on all returned data storage devices. While Staples had enhanced its procedures and control mechanisms in response to the complaints, our audit found that they have not been effective in all cases since then. In summary, the deficiencies which existed in 2008 persist today, continuing to place personal information at risk. Until this matter and the other recommendations in this report are addressed, Staples will not meet its obligations under *PIPEDA*.³⁸⁹

Upon publication of the Annual Report, this finding occasioned much discussion. For the purposes of this discussion, I want to highlight two different responses to the report, both found in comments by readers of a well known academic blog by leading Internet law scholar, Michael Geist. While one commentator expostulates that:

Staples not at fault for their customers' failures

1. Customer buys electronic device featuring data storage medium from Staples.
2. Customer puts their personal, private info on data storage medium.
3. Customer returns the electronic device to Staples WITHOUT FIRST removing THEIR OWN personal, private information form data storage medium THEMSELVES.

³⁸⁹ Office of the Privacy Commissioner of Canada "Chapter 3: Destruction of Data in the Digital Age" *Annual Report to Parliament 2010: Report on Personal Information Protection and Electronic Documents Act* online: <http://www.priv.gc.ca/information/ar/201011/2010_PIPEDA_e.asp#sect5>.

4. Staples accepts the return, presumably determines it's not actually defective, and puts it back on the shelf to be sold again.

Never at any point in this process did the customer give Staples their private information for safe-keeping. Staples SHOULD NOT have any obligation here whatsoever to protect customer information (aside from any credit/debit/payment card details and any associated info related to the purchase), because their customer haven't provided them with any. These customers whose info was found on devices on Staples' shelves PUT THAT INFO ON DEVICES WHICH THEY OWNED! Then they failed to remove that info from DEVICE WHICH THEY OWNED before they LET SOMEONE ELSE OWN THE DEVICE.

Staples DID NOTHING WRONG!!! THEIR MORON CUSTOMERS DID!³⁹⁰

Another commentator counters with the opinion that:

While I agree with you that there are a lot of "morons" with purchasing power, I don't agree that Staples could not do anything about it.

Although strictly speaking they shouldn't be "responsible" for morons, they can implement some measures to help mitigate their lack of actions. Even a simple checkbox question on the return form that asks "have you removed all personal information from this device?" would go a long way towards being proactive. If the answer is "no" (or unknown), then Staples staff would know they may need to take further actions.³⁹¹

³⁹⁰ Mr. Nerdly @ <<http://www.michaelgeist.ca/content/view/5880/125>>. Recalling discussions in Part I about how mainstream expectations built into responses may disempower Others, notice how the stupid user blaming around the Staples issue could have other resonances: a gendered 'stupidity' where the customer was female and less technologically sophisticated; a classist or racialized 'stupidity' where lack of education, leisure time, or knowledge played into the failure to erase the hard drive. This is not to say that these are necessarily present in this response, but simply to call attention to the way(s) in which the 'stupid user' responses may also act to disempower already Othered groups further.

³⁹¹ Oldguy @ <http://www.michaelgeist.ca/content/view/5880/125>.

B: NATHALIE BLANCHARD

Ms. Blanchard is the Quebec woman discussed earlier, the one whose sick benefits were terminated by Manulife.

Ms. Blanchard was an IBM employee who was diagnosed with major depression. She was on sick leave and receiving disability payments for a year and a half. During that time, Ms. Blanchard attended therapy and took medications as prescribed. Eventually, her psychiatrist suggested that she try taking a trip. Allegedly she then booked the trip, notified her insurance company, and on her return posted pictures from the trip(s) to Facebook. Her Facebook account is set to “private”.

Her insurance company, Manulife, does not deny terminating her benefits, nor that information from her social media profile was involved in the decision. They do, however, state that “We would not deny or terminate a valid claim solely based on information published on Web sites such as Facebook.”

Ms. Blanchard is currently pursuing a remedy in court.³⁹²

Despite the fact that Ms. Blanchard was travelling under medical advice, many of the comments on the news story seem to start from the assumption that either Ms. Blanchard was simply caught defrauding insurance or, best case, that she was foolish to behave publicly in ways that were inconsistent with depression and that by so doing she had opened herself to termination of her benefits.

C: CORPORAL BROWN

A staged photo series of an abduction scenario was posted on the FetLife.com³⁹³ website. The man in the photographs was identified as RCMP Corporal Jim Brown.

³⁹² The proceedings are apparently ongoing as at 13 March 2012.

³⁹³ FetLife.com is a private website that positions itself as being for the kink and BDSM communities. Content on the site is viewable only by members of the site. The Terms of Use s.4, USER CONDUCT,

Issues were raised about the photo series content as well as Corporal Brown's participation on the site itself.

Corporal Brown's Detachment Commander investigated the allegations and concluded that: "[t]he alleged issue was deemed to be off-duty, non-criminal, adult consensual activity during which the individual was not representing himself as a member of the RCMP and thus it did not appear to legal services to meet the threshold for a code-of-conduct violation.,"

Despite this finding, a week later the Acting Commanding Officer of the BC RCMP announced that both an internal code of conduct investigation and an independent investigation had been initiated.³⁹⁴

In this story, there are actually two levels of inference and commentary taking place. First of all, despite the original conclusion that Corporal Brown's participation on the site was entirely separate from his identity as an RCMP officer and thus there had been no violation of the code of conduct, the initiation of further investigations by the Acting Provincial Commander of the RCMP is indicative of a belief that the off-duty online behaviour was relevant, a conclusion further bolstered by the Acting Commander's comment that "While we must strike a balance between an individual's rights and freedoms when off-duty and the RCMP code of conduct, I am personally embarrassed and very disappointed that the RCMP would be, in any way, linked to photos of that nature." A second level of scrutiny of the behaviour comes in the comments to the news

stipulates, among other things, that Users not take any content out of the site and re-post or use elsewhere without explicit written permission of the user to whom it relates.

<<https://fetlife.com/fetlife/tou>>.

³⁹⁴ Interestingly, despite the fact that one day after the announcement of the further investigations evidence surfaced showing that Corporal Brown was NOT the individual in the photographs <<http://eroticvancouver.com/spotlight-on-the-media-abduction-scene-photos-are-not-of-rcmp-corporal-brown>> the investigations continued, simply with a broader focus, looking at his involvement with the site and BDSM generally rather than the photo series specifically.

story³⁹⁵, which are extensive. In that arena, it is noteworthy that even where the commenter argues that Corporal Brown's sex life has nothing to do with his employment, many of them then continue on to critique the decision to post photos and/or to participate publicly on a site such as Fetlife.com.

WHY ARE THESE USERS "STUPID"?

- A. Individuals who return technology to a retail organization are considered to be "stupid" for trusting that the organization was acting in compliance with Canadian law and their own policies;
- B. A woman acting on medical advice and posting pictures that she designated as "private" on Facebook is "stupid" for not hiding her activities; and
- C. A man participating on a membership-only site in his off-work hours and with no identification of himself as affiliated with the RCMP is "stupid" for endangering his career.³⁹⁶

It is my contention that the stupid user meme has a function, that this isn't a mere difference of opinion about privacy. Rather, the stupid user meme functions to simultaneously reinforce understanding of the perils of online spaces for personal

³⁹⁵ There are multiple comments and perspectives available through a perusal of the comments on news stories about Corporal Brown's situation. Leaving aside the discussions about BDSM practices themselves, the "stupid user" indictment is still evident. See for example Izolnirt's comment on the CBC article that "What two consenting adults do in their bedroom should be no one's business. On the other hand, this officer was clearly asking for it, by allowing his private activity to become public, by way of posting photographs on the internet, assuming it wasn't his female partner who did it without his permission. That, rather than his kinky tastes, should make everyone question his competence judgement". Commenter A Priori takes the similar position that "I don't think there's a problem with anything done between consenting adults but I am never going to understand the need to take pictures of oneself doing it and then post them on any website. Especially when it is something that could come back and bite you in the backside." <<http://www.cbc.ca/news/canada/british-columbia/story/2012/07/05/bc-rcmp-sex-photos.html>>

³⁹⁶ In this particular case, there ultimately appeared to be no conflict between Cpl. Brown's activities and his employment. It is interesting to speculate what would happen in a similar situation where there was a conflict but the activity still took place in off-work hours. Is an individual 'stupid' to have a personal life? What are the implications of learning about private activities of a public servant where those activities do intersect with the duties of that person?

information and reputation control while locating blame at the level of individual error rather than as endemic to the spaces and processes themselves. Locating the problem this way allows public discussions about risks that effectively raise population anxiety and exacerbate the sense of risk upon which the government, administrative and economic policies and enterprises are based. At the same time, even while raising the general level of anxiety, the “stupid user” allows those of “us” who have been “properly” responsabilized into acting in the expectedly vigilant manner and using the various legal, administrative and commercial tools provided, to feel that “we” are secure (and thus to continue our online participation) even as we decry the risks of those spaces generally. That security is, of course, illusory; not only does it encourage reliance on the idea that only the “stupid user” is at risk, but it also sets up a situation where no further inquiry is needed, leaving the corporate aims designed into the system unexamined.

In order to make this case, in the sections that follow, I will discuss: the process of governmentality and how it shapes not only policies and laws but the experiences of citizens; a shifting relationship between citizens and governing bodies towards the responsabilization of ordinary citizens; and then examine the relationship(s) between government, responsabilization and the regulation of persons via reputation.

Law & Society

In a 1990 interview with Tony Negri, Gilles Deleuze commented that “what interests me isn’t the law or the laws (the former being an empty notion, the latter uncritical notions), nor even law or rights, but jurisprudence. It is jurisprudence ultimately that creates law, and we mustn’t go on leaving this to judges.³⁹⁷”

Those with legal training understand the term “jurisprudence” as meaning the body of case law produced by courts; the interpretation of laws. However, given that Deleuze explicitly says that we must go beyond the judicial, the term clearly must be more broadly understood. The American Heritage Dictionary defines the term as meaning

³⁹⁷ Gilles Deleuze, *Negotiations, 1972-1990*, trans. by Martin Joughin (1990) at 169

“the science of philosophy of law”³⁹⁸, which may be applicable but still seems quite restrictive for something a generic “we” are being encouraged to participate in. Instead, Deleuze’s comment should best be understood as indicating a definition of jurisprudence that is more extensive: “Jurisprudence implies creating a body of law and methods for interpreting the law, studying the relationships between law and society, and predicting the effects of legal decisions.”³⁹⁹

A useful example of this approach can be found in Garland’s study of crime control in the US and UK. In the introduction, he writes:

The roots of today’s crime control arrangements lie in the character of contemporary social organization and the political and cultural choices that have been made in relation to it. And the new world of crime control provides, in its turn, important sources of legitimation for an anti-welfare politics and for a conception of the poor as an undeserving underclass. The mutually supportive character of today’s penal and welfare policies – based on principles that are quite different than those described in Punishment and welfare – is indicated by an analysis of the discursive tropes and administrative strategies that run through both of these institutional domains.⁴⁰⁰

To apply the jurisprudential approach endorsed by Deleuze to the question of reputation, then, requires an examination of the social organizations, political and cultural choices that are being made around issues of reputation.

Governmentality

What I am talking about might be described as governance; not merely in the sense of the study of the government itself, but rather in terms of the exercise of control(s) in shaping citizens, policies and laws. Although Michel Foucault first coined the term

³⁹⁸ Dictionary.com, s.v. “Jurisprudence” (2004).

³⁹⁹ *Ibid.*

⁴⁰⁰ David Garland, *The Culture of Control: Crime and Social Order in Contemporary Society* (Chicago: University of Chicago Press, 2001) at xii

“governmentality”, the term and its underlying meaning(s) have been the basis both of critique and expansion by other theorists.⁴⁰¹

Foucault used the term “governmentality” to mean three things:

The ensemble formed by the institutions, procedures, analyses and reflections, the calculations and tactics that allow the exercise of this very specific albeit complex form of power, which has as its target population, as its principal form of knowledge political economy, and as its essential technical means apparatuses of security.

The tendency which, over a long period and throughout the west, has steadily led towards the pre-eminence over all other forms (sovereignty, discipline, etc) of this type of power which may be termed government, resulting, on the one hand, in the formation of a whole series of specific governmental apparatuses, and, on the other, in the development of a whole complex of saviours.

The process, or rather the result of the process, through which the state of justice of the Middle Ages, transformed into the administrative state during the fifteenth and sixteenth centuries, gradually becomes ‘governmentalized.’⁴⁰²

Parsing this definition, it appears that Foucault uses “governmentality” as a process rather than an object; that it refers, ultimately, to the way(s) government works within

⁴⁰¹H Hunt & G Wickham, *Foucault and Law* (London: Pluto Press, 1994);D Kerr, "Beheading the King and Enthroning the Market: A Critique of Foucauldian Governmentality" 63:2 *Science & Society* (1999) at 173; and M. Dean, *Governmentality: Power and Rule in Modern Society* (London: Sage, 1999) have all addressed the idea of governmentality and its implications in different ways. The work of Thomas Lemke, "Foucault, Governmentality, and Critique" *Rethinking Marxism*, 14:3 (2002) 49, provides a bridge between explorations of governmentality and towards understandings built upon and expanding on means of governance in various areas. Best known, perhaps, are Nikolas Rose, *Powers of Freedom: Reframing Political Thought* (Cambridge: Cambridge University Press, 1999),Nikolas Rose & Peter Miller, "Political Power Beyond the State: Problematics of Government" *British Journal of Sociology* 43:2 (1992) 173;Barbara Cruikshank, *The Will to Empower: Democratic Citizens and Other Subjects* (Ithica London: Cornell University Press, 1999), and Paul Henman, "Targeted! Population Segmentation, Electronic Surveillance and Governing the Unemployed in Australia" *international Sociology* 19:2 (2004) 173.

⁴⁰² Michel Foucault, "Governmentality", Graham Burchell, Colin Gordon & Peter Miller eds., *The Foucault Effect: Studies in Governmentality* (Chicago: University of Chicago Press, 1991) 87 at 103.

the larger political economy to achieve its goals, a process that has had many forms historically. Or, as Fusco (invoking Rose) puts it "...all those more or less rationalized programs, strategies and tactics for the conduct of conduct, for acting upon the actions of others in order to achieve certain ends."⁴⁰³

In order to understand current governance strategies, then, it is necessarily to identify what the aims or ends the process seeks to instantiate and encourage actually are. Recalling the earlier discussion of risk and risk societies, I would suggest that the aims/goals in this area be best understood looking through the lens of "security". Arguably, of course, security has always, to some degree, been the goal of governing bodies, but in the modernist risk society the impetus towards security has become more pronounced even as uncertainty has grown. Giddens would suggest that at its most basic the focus on security is very much linked to the risk society, and further that "as we move towards a world dominated by manufactured rather than external uncertainty, there is a renewed discussion of the nature of responsibility."⁴⁰⁴

Responsibilization

Taking security as the end towards which governance is shaped and shaping, it is necessary next to examine what approach is being taken to arrive there; what approach is being shaped and how responsibility is implicated within it.

Rose identifies an important shift in the relationship between the populace and the governing body, a shift that he sees as part of the move towards modernity. In this shift, "the ideal of an omniscient social state that would shape, coordinate and manage the affairs of all sectors of society has fallen into disrepute."⁴⁰⁵ He suggests that in this shift, people's identification and allegiance has changed; no longer the overarching

⁴⁰³ Caroline Fusco, "Inscribing Healthification: Governance, Risk, Surveillance and the Subjects and Spaces of Fitness and Health", *Health and Place* 12 (2006) at 68

⁴⁰⁴ Anthony Giddens, "Risk and Responsibility" *The Modern Law Review* 62:1 (1999) at 7

⁴⁰⁵ Nikolas Rose, "The Politics of Life Itself" *Theory, Culture & Society* 18:6 (2001) at 5

social contract between the individual and the State, but instead a multiplicity of relational identities and community memberships, forming a net of obligations.⁴⁰⁶

Such a shift would signal a move from the traditional hierarchal structure, where power is exercised downwards, by the rulers over the ruled, towards a more all-encompassing structure of power.⁴⁰⁷ As for what that broader structure might look like, Rose suggests that “we are seeing the emergence of a range of rationalities and techniques that seek to govern without governing society, to govern through regulated choices made by discrete and autonomous actors in the context of their particular commitments to families and communities.”⁴⁰⁸

Obviously, “acting upon the conduct of others” can take many forms, indeed, virtually any regulatory action or exertion of force by government falls under that rubric. Understanding governmentality requires something more, however; acting upon the conduct of others in such a way as to maximize the desired result and minimize the necessity of exerting force or coercion takes us, in turn, to the idea of responsabilization.⁴⁰⁹

At its most basic, responsabilization refers to the offloading of governmental responsibility to individual actors. That is, just as Rose saw a shift from the allegiance to an overarching nation-state, so too does responsabilization contemplate a shift from citizen dependence on the State into citizens being made responsible for themselves and acting accordingly. The move to responsabilization should not, however, be

⁴⁰⁶ Nikolas Rose, “The Politics of Life Itself” *Theory, Culture & Society* 18:6 (2001) at 5

⁴⁰⁷ *Ibid.*

⁴⁰⁸ Nikolas Rose, “The Death of the Social? Re-Figuring the Territory of Government” *Economy and Society* 25:3 (1996) at 328

⁴⁰⁹ Most notably, Thomas Lemke recognized the role of responsabilization in neo-liberal governance, describing it as the process of leading citizens/subjects to see social risks (for instance illness, poverty, unemployment) as falling within the sphere for which the individual rather than the State is responsible, and by so doing transform such issues into a problem of self-care. Thomas Lemke, “The Birth of Bio-Politics: Michael Foucault's Lectures at the College de France on Neo-Liberal Governmentality” *Economy and Society* 30:2 (2001) 190 at 201

mistaken as reductive of State power. Rather, it indicates a move towards a seemingly dispersed culture of power that, ultimately, is still shaped and overseen by government and works to support the aims/ends identified by governing bodies. In order to do so, all players within the culture experience changes in approach and attitude; governments, administrative institutions, commercial entities, communities and families are all engaged in a cognitive shift. The shift itself is, to some extent, self-reflexive, that is, changes to rhetoric and values towards a greater focus on individual power and responsibility leads to a governing body that espouses these commitments. The programs and approaches in which that governing body invests will in turn both build on the individual focus and, in so doing, support and perpetuate the faith in it.

Let us return quickly to the three examples already discussed:

- A. Staples: despite the existence of law and policies at multiple levels regulating how the organization is required to deal with the personal information of consumer's, the focus of the discussion becomes the actions (or lack thereof) of the consumer in failing to protect their own information. Government, the organization, and the media – all focus on individual responsibility.
- B. Nathalie Blanchard: An individual who acts in conformance with medical advice and posts related information and photos on an online site (one that has a Terms of Use that specifically limits the uses to which information on the site may be used) loses her disability benefits due to inferences drawn by the insurance company based on that information and those photos. Again, the discussion doesn't focus on the appropriateness of the insurer's action or even the role of a corporation whose business model is based on eliciting and encouraging disclosure of personal information in order to exploit it. Instead, all attention gets levied at the merits or lack thereof of Ms. Blanchard's decision to put such information online. Again, despite the situation involving an employer, an insurance company, personal health information and government and corporate interests in the SNS site, the

responsibility in this case is being focussed on the individual affected and her responsibilities.

- C. Corporal Brown: RCMP officer is suspended from the force and subjected to multiple investigations and media attention after sexually explicit photographs in which he allegedly appears are posted on a membership only sexual fetish website. Multiple discussions spring from this but they are almost all focussed on the appropriateness of the officer's actions – participation in BDSM, photographing private practices, or posting the information on a website – rather than on the fact that participation in and photographs of participation in legal, consensual activities in one's off-work hours should not be open to review or inspection by employers or the media. Criminal law, a federal employer, administrative bodies and multiple forms of media are all implicated in various aspects of the situation, yet the responsibility question is almost entirely focussed on the actions of the individual.

Speaking of crime control, Garland notes that

...institutions of crime control and criminal justice have definite conditions of existence. They form part of a network of governance and social ordering that, in modern societies, includes the legal system, the labour market and welfare state institutions. They refer to and are supported by other social institutions and social controls, and are grounded in specific configurations of cultural, political and economic action.⁴¹⁰

Similarly, when exploring responsabilization, we are not looking at a binary opposition of individuals versus State responsibility, instead, there is a network of laws, institutions and messages, all of which combine to encourage individual agency and

⁴¹⁰ David Garland, *The Culture of Control: Crime and Social Order in Contemporary Society* (Chicago: University of Chicago Press, 2001) at 5

responsibility within the bounds desired (and set) by various⁴¹¹ governing bodies. In each of the situations I have discussed, this process is evident.

One offshoot of responsabilization can be seen in a phenomenon sometimes referred to as healthification or healthism.⁴¹² For example, in the context of university locker rooms, Fusco notes that “the occupational health and safety regulations and the university experts, then, assist in the process of self-governance through the rules, regulations, guidelines and advice they offer, which are supposed to facilitate the taking up of the healthiest choice. The rules and regulations can be thought of as technologies of normalization: they provide a set of norms for behaviour...which render citizens active and productive in the exercise of those norms.”⁴¹³ In the case of the locker room, Fusco was examining a network of administration; from occupational health and safety law; through university and building policies which were developed to enhance and encourage compliance with those laws; through to norms and expectations of users. All these together combined to create the technologies of normalization she identifies; the development, dissemination and reinforcement of norms of behaviour to which the individual is then expected to adhere.

⁴¹¹ In part I, I discussed the way mainstream values can have a governance effect in social interactions, as well as the way that site designers can build governance expectations right into the code. Above these levels, of course, are other perhaps more recognizable forms of governance, but it would be a mistake to discount these.

⁴¹² Healthification may be understood as an offshoot of the responsabilization discourse, one that is focussed on health. Nikolas Rose has applied his governmentality understanding to describing it as a process wherein “public objectives for the good health and good order of the social body with the desire of individuals for health and well-being”. Theorists disagree on the process by which this takes place, with some describing it as a kind of soft paternalism or even totalitarianist coercion [Petr Skrabanek, “The Death of Humane Medicine and the Rise of Coercive Healthism” *Social Affairs*, (1994)], keying on governmentality, Rose insists that no coercion or force is needed to transfer these goals to citizens, rather that people want to be healthy and thus take on the responsibility for being so.

⁴¹³ Caroline Fusco, “Inscribing Healthification: Governance, Risk, Surveillance and the Subjects and Spaces of Fitness and Health”, *Health and Place* 12 (2006) at 73

Nor are various levels of government and administrative rules the only way(s) in which this process of normalization works. As will be seen⁴¹⁴ in discussions of insurance and security, commercial interests and entities also play a part in this process, offering products that appear to facilitate individual agency even while their existence acts to reaffirm the individual belief in the necessity of action. Again, these commercial entities should not be seen as somehow diminishing or usurping the role of the State, rather, even while commercial actors function, it is the State in the background that licenses and approves, thus implicitly shaping and regulating the behaviour of commercial entities even as it appears to step back and waive responsibility.⁴¹⁵

Take as an example insurance companies. They offer a variety of products; home insurance, auto insurance, even life and health insurance. These products are not offered in a vacuum, and indeed chaos would result if they were.⁴¹⁶ In order to show the interplay between government, commercial interests and individuals, let's explore automobile insurance, since it differs from other forms of insurance by being mandatory in Canada. Though mandatory, auto insurance requirements are set by provinces and territories and vary accordingly, from provinces where insurance is primarily provided by provincial bodies themselves (BC, MB, SK), to provinces where private companies provide the coverage. Regardless of how this happens, the (federal)

⁴¹⁴ See for example David Garland, *The Culture of Control: Crime and Social Order in Contemporary Society* (Chicago: University of Chicago Press, 2001) at 203; Anthony Giddens, "Risk and Responsibility" *The Modern Law Review* 62:1 (1999); Francois Ewald, "Insurance and Risk" Colin Graham, Graham Burchell & Peter Miller eds., *The Foucault Effect: Studies in Government Rationality* (1991) 197

⁴¹⁵ David Garland, *The Culture of Control: Crime and Social Order in Contemporary Society* (Chicago: University of Chicago Press, 2001) at 2003. The role of the State in approving may not be active; the decision not to regulate or enter a particular space may itself be an act of approval, allowing existing power relations or structures to remain undisturbed.

⁴¹⁶ Terry Pratchett, in an early Discworld novel, describes insurance as a process whereby you bet with the bank that your house will burn down and the bank bets that it won't. Unsurprisingly, within such a scheme, the city of Ankh-Morpork goes up in flames as all who have bought insurance begin to torch their homes to recoup costs. There must, therefore be limits on what insurance covers in order for it to be an effective business model. Similarly, if consumers purchased insurance but did not receive the coverage to which they were entitled, then consumers would fairly quickly lose faith in the notion of insurance, cease to invest in it, and again the efficacy of the business model terminates.

Office of the Superintendent of Financial Institutions monitors all insurance companies within Canada to ensure that they hold appropriate capital to cover policies sold and to ensure that investments made by the company are prudent.⁴¹⁷ Additional government regulations cover the licensing of insurance agents and oversee the setting of insurance rates and what factors may be used in such assessments.

Insurance, then, involves interrelated roles of the State, administrative bodies and commercial bodies. Responsibilization, however, takes us inevitably to the individual and individual agency as part of this equation. Where social and political norms, hard law (laws), soft law (policies and procedures), and economic incentives can encourage individual responsibility, in the end it works only if the individual does indeed become a willing⁴¹⁸ participant in the process. That is, effective responsibilization requires not simply the participation by the individual, but uptake⁴¹⁹ by that individual. Insurance companies offer multiple forms of insurance, all intended to further the goal of security and exhibiting this web of governance forces and individual responsibility.

How then is uptake grounded or encouraged? With regard to insurance, Rose talks about security in multiple ways. Security and insurance, for instance, demonstrate how individuals are encouraged⁴²⁰ to be responsible for their own security through health

⁴¹⁷ Interestingly, the requirement that investments be prudent and quickly liquidate-able results in insurance companies being major investors in federal, provincial and municipal bonds. This creates a further interdependency between commercial entities and governing bodies.

⁴¹⁸ Willingness, however, does not preclude some aspect of coercion. When I speak of willing participation, I do not necessarily mean active and enthusiastic agreement so much as an incorporation and internalization of the expectations.

⁴¹⁹ Marilyn Frye discusses uptake as responding to the anger of another person in a way that addresses the implicit claims that they are making in their expression of anger: Frye, "A Note on Anger" *The Politics of Reality* (Trumansburg, NY: Crossing Press, 1983) at 89. As such, uptake is predicated on respect, understanding and acceptance of the perceived legitimacy of the claims being made. In this case, that means not only that an individual participates in the process but that the individual internalize and accept as worthy the propositions upon which the process is predicated.

⁴²⁰ The 'encouragement' may have different degrees of coercive power, up to and including a requirements in the case of auto insurance, which is mandatory in Canada. Nevertheless I contend that the field of insurance does work to show responsibilization in action.

insurance, pensions, property insurance, etc.⁴²¹ In terms of bodily and property security, Rose identifies still more individual and community-driven moves towards responsibility for safety; gated living communities, shopping malls with private security, etc.⁴²² Garland demonstrates how shifts in crime control and policing are grounded in a rhetoric where “offenders must be deemed to be free, to be rational, to be exercising choice, because that is how we must conceive of ourselves.”⁴²³ Focussing on health, Fusco demonstrates how “people transform themselves into subjects of self-regulation within the discourses of risk and the new public health. Individuals police themselves and exercise power on themselves; they are interested in the pursuit of self-improvement, happiness and health.”⁴²⁴

While these various approaches and bodies encourage individual responsibility, there is something more motivating individuals to give those ideas uptake. The key, I believe, is a set of social and political norms that do not merely encourage responsibility but actually set it up as a moral imperative, part of an implicit social contract.

Ewald identifies insurance as a “moral technology...no longer resigning oneself to the decrees of providence and the blows of fate, but instead transforming one’s relationships with nature, the world and God so that, even in misfortune, one retains responsibility for one’s affairs by possessing the means to repair its effects.”⁴²⁵ Fusco identifies something similar within healthification, noting that “risk-avoidance behaviour...becomes viewed as a moral enterprise relating to issues of self-control, self-knowledge and self-improvement. It is a form of self-government, involving the

⁴²¹Nikolas Rose, "The Death of the Social? Re-Figuring the Territory of Government" *Economy and Society* 25:3 (1996) at 341.

⁴²² *Ibid.*

⁴²³ David Garland, *The Culture of Control: Crime and Social Order in Contemporary Society* (Chicago: University of Chicago Press, 2001) at 198.

⁴²⁴ Caroline Fusco, "Inscribing Healthification: Governance, Risk, Surveillance and the Subjects and Spaces of Fitness and Health", *Health and Place* 12 (2006) at 70

⁴²⁵ Francois Ewald, "Insurance and Risk" *The Foucault Effect: Studies in Government Rationality*, edited by Colin Graham, Graham Burchell and Peter Miller (1991) at 207.

acceptance and internalization of the objects of institutional government."⁴²⁶ Although he eschews the term morality, Rose too identifies a process whereby the focus on security and risk-management creates an environment where the individual is obligated to become a responsible actor; "the ethics of lifestyle maximization, coupled with a logic in which someone must be held to blame for any event that threatens an individual's quality of life, generates a relentless imperative of risk management not simply in relation to contracting for insurance, but also through daily lifestyle management, choices of where to live and shop, what to eat and drink, stress management, exercise and so forth."⁴²⁷ This creates, then, the responsibility of the individual to act, transformed by social, political and economic messages into a (moral) imperative not only to act but to act in a certain way.

Responsibilization then means acting upon the conduct of others in such a way as to maximize the desired result and minimize the necessity of exerting force or coercion. In this case a key ideological investment is the liberal fetishization of individual responsibility, which is encouraged via responsibilization. That is, power is dispersed and operates in a diffuse manner through a variety of different institutions and connections – government, administrative bodies, commercial enterprises and individuals – all creating, and promulgating, policies and approaches that intersect and mutually support each other in bolstering the foundational notion of individual responsibility and ultimately in instantiating a culture of individual responsibility.

Within this framework of responsibilization, the individual internalizes the idea that her role in the social contract requires not just civic participation but a risk-management, self-directed moral imperative to manage her own behaviour. As part of this social contract, s/he also takes on the responsibility of monitoring the actions of others and making that information available in order to facilitate the risk-management

⁴²⁶ Caroline Fusco, "Inscribing Healthification: Governance, Risk, Surveillance and the Subjects and Spaces of Fitness and Health", *Health and Place* 12 (2006) at 70

⁴²⁷ Nikolas Rose, "The Death of the Social? Re-Figuring the Territory of Government" *Economy and Society* 25:3 (1996) at 342

assessments of others. It is at this point that reputation becomes an important part of the framework; reputation is the means by which we surveil each other, effectively shaping and policing behaviour, access to services, and information. Reputation then is the most granular level of responsabilization, its active iteration at the individual level, and the stupid user is the individual who fails to uphold her (moral) responsibility to act in both the expected and acceptable way, not only for her own purposes but to facilitate the larger purposes of the liberal State.

Reputation and Responsibilization

Having sketched out an approach to governmentality and responsibility, I turn now to the question of whether and how these factors are at work in regulation of and by reputation. I will do so by examining each field individually – governmental messages expressed in law; administrative messages and policies; economic and commercial factors; and finally individual rhetoric and expectations – to make evident how the process of responsabilization is functioning here.

Canada's private sector privacy law (PIPEDA⁴²⁸) – the legislation that governs the area – contains a public education mandate⁴²⁹ and is complaint-driven, both clear indications of an expectation of individual agency. The messages and policies being disseminated by administrative bodies support this expectation, speaking about the dangers of personal information in online spaces, urging users to be aware of what information about them is online and to be judicious in what information they make available. The commercial sector has a variety of tools that assist users with this enterprise, allowing them to monitor their online presence, with an obvious eye to identifying and “fixing” negative reputation factors, either via the service or autonomously, by the individual. At every stage of the political, social and economic process, the norms and expectations reaffirm that personal information, identity

⁴²⁸ *Supra* note 241.

⁴²⁹ Indeed, beyond the active education mandate, it could be argued that much of PIPEDA's structure is about giving the individual information upon which to act in order to protect her personal information, thus still encouraging the idea of individual responsibility.

performance and reputation online are risks, and provide tools and encourage individuals to protect themselves vigilantly against these risks by every means available.

GOVERNMENT

Currently, there is limited government regulation of reputation at a criminal level, except that which focusses on the fraudulent misuse or theft of personal identity information.⁴³⁰

Amendments to the *Criminal Code* in 2009 also added a specific section dealing with Identity Theft and Identity Fraud.⁴³¹ The federal *Employment Insurance Act* contains similar provisions related to the Social Insurance Number.⁴³² There are also some provisions in provincial legislation, though again none specifically directed at identity. In so far as there is law that may be applicable to the development, collection and use of reputation, it is the privacy laws of Canada; the public sector *Privacy Act*⁴³³ and the private sector *PIPEDA*.⁴³⁴

Regulation of reputation must include some form of control over personal information of and about an identifiable individual. This kind of informational self-control has been, at least arguably, translated into the data protection approach. Data protection is very much a product of the technologies it seeks to address. In the 1960s and 70s, as

⁴³⁰ *Criminal Code of Canada*, Fraud (s. 380); obtaining credit by false pretence or fraud, or knowingly making a false statement with the intention that it be relied upon in order to secure property, money, loan, credit, etc (s. 362); forgery (s. 366-378); theft, forgery etc of credit card (s. 342); making, executing, drawing, signing, accepting or endorsing a document with intention to defraud (s. 374); forgery or uttering a forged identity document (s. 56.1); forgery or uttering a forged passport (s. 57); personation with intent (s. 403); fraudulently obtains, uses, utters, traffics in or permits the use of credit card data and authentication information (s. 342(3)); and unauthorized use of computer (s. 342.1).

⁴³¹ S. 401.1, 401.2, and 403. <http://www.parl.gc.ca/HousePublications/Publication.aspx?Doc=S-4_4&File=27&Language=E&Mode=1&Parl=40&Pub=Bill&Ses=2>.

⁴³² *Employment Insurance Act* (S.C. 1996, c. 23) <<http://laws-lois.justice.gc.ca/eng/acts/E-5.6/>>

⁴³³ *Supra* note 323

⁴³⁴ See discussion in chapter 5 on applicability of these Acts to reputation at page 139

information technology developed and advanced, public and private organizations were able to process ever-increasing amounts of information about individuals. As people became increasingly concerned about their ability to protect their privacy, states began to recognize and attempt to govern such activities.⁴³⁵ However, where a rights-based approach focusses on the dignity and autonomy of the individual, data-protection focusses rather on regulating the information, intending thereby to reduce or manage damage to individuals caused by misuse or disclosure of that information. Review of both the Privacy Act and *PIPEDA* show an adherence to this idea of personal information and informational self-determination. Of particular interest when considering this question of governance and responsabilization, however, are the infrastructures set up explicitly and implicitly by the legislation.

It should be noted at this stage that neither a data protection nor a rights-based approach to legislation is fully applicable to reputation due to their narrow focus. As explored in Part I of this dissertation, reputation is a complex social concept, one that cannot be fully (or even adequately) addressed by focussing only on the information.⁴³⁶ Nevertheless, since data protection is the most applicable approach extant, this section will use that approach as an example to show the responsabilization process.

This section will examine the development and drafting of *PIPEDA* in order to show the interrelationship between government, commercial entities and the individual. Privacy has historically been conceptualized as a right, and linked with notions of dignity and

⁴³⁵Roger Clarke, "Beyond OECD Guidelines: Privacy Protection for the 21st Century", online: <www.rogerclarke.com>. Clarke notes "The first laws that expressly protected information privacy were passed in Europe in the early 1970s. The West German Land of Hesse passed its Datenschutzgesetz (Data Protection Act) in 1970, and that term quickly came to be used in virtually all discussions. Sweden's Data Act of 1973 was the first such legislation at national level. A succession of Continental countries followed, including Germany in 1977 and France in 1978."

⁴³⁶ For instance, some form of equality or rights-based protection would also be necessary in order to protect against the collection of some information and against some inferences drawn from reputation information.

autonomy.⁴³⁷ Canada's earliest moves in privacy regulation were in accordance with this; in 1977 Canada introduced data privacy provisions into the *Canadian Human Rights Act*. These provisions covered information on natural persons that was held by the federal government and had been used in making decisions about the individual concerned.

Although Canada's first moves on this issue were clearly grounded in the rights tradition, the approach began to vary. Advocacy to include a right of privacy in the Canadian *Charter of Rights and Freedoms* was unsuccessful⁴³⁸, and the repeal of Part IV of the *Human Rights Act*⁴³⁹ and passing of the *Access to Information* and *Privacy Acts* in 1983⁴⁴⁰ signalled a shift from a purely rights-based approach to privacy to a more data-protection grounded approach.

As state- and country-specific data protection laws were enacted, concern arose that disparate national data protection schemes could hinder the free flow of information across borders, causing disruptions in important sectors of the economy. Accordingly, both the Council of Europe and the Organization for Economic and Cultural Development (OECD) created documents which set out fair information principles and attempted to harmonize trans-border data flow issues by setting standards of co-operation, consultation and assistance. These principles were expected to form a template for national legislation.⁴⁴¹

⁴³⁷ See Article 12 of the *Universal Declaration of Human Rights* (1948) or Article 17 of the 1966 *International Covenant on Civil and Political Rights*.

⁴³⁸ *Canadian Charter of Rights and Freedoms*. Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11. Privacy is not entirely excluded from the purview of the Charter – some limited privacy interests have been found to be protected under sections 7, 8 and 2(b) of the Charter.

⁴³⁹ *Canadian Human Rights Act* (R.S.C., 1985, c. H-6). This law, when originally passed in 1977, included as Part IV Canada's first public sector privacy protections.

⁴⁴⁰ *Privacy Act*, R.S.C. 1985, c. P-21; *Access to Information Act*, R.S.C. 1985, c. A-1. When these Acts came into force, Part IV of the *Canada Human Rights Act* was repealed.

⁴⁴¹ See Preface, Organisation for Economic Cooperation and Development, *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, 23 September 1980, available at: <http://www.unhcr.org/refworld/docid/3dde56854.html> [accessed 16 December 2012]

The OECD Guidelines were non-binding, and not all European nations ratified the Council of Europe Convention. Accordingly, in 1990 the European Union began working towards an EU Directive on data protection, and in 1995 the European Union formally adopted a directive⁴⁴² predicated on fair information principles.

Canada became a signatory of the OECD Guidelines in June 1984. These Guidelines were not binding, however, and while some industries developed some form of fair information principles,⁴⁴³ there was no substantial private sector movement towards private sector privacy until the 1990s, when the European Union Directive was proposed and lawmakers and industry representatives became concerned about the impact of the Directive. Of particular concern were the standards imposed in that document regarding trans-border flows of data, where the data could only be transferred to a third country where that country is recognized as providing an adequate level of data protection.⁴⁴⁴ Fears about the impact of these provisions galvanized a Canadian move towards developing some form of private sector privacy regulation.

In the 1990s, the Canadian Standards Association began to organize around the issue and discussed the development of a standard for data protection. They formed a committee made up of consumer representatives, business representatives, interested organizations (such as labour unions and professional associations) and

⁴⁴²European Union, *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, 24 October 1995, available at: <http://www.unhcr.org/refworld/docid/3ddcc1c74.html> [accessed 16 December 2012].

⁴⁴³ For instance, credit reporting legislation enacted in the 1980s granted consumers the right to access and correct their credit information. In another section, the Canadian Bankers Association adopted a model Privacy Code for individual customers in 1990 that was based on the OECD Guidelines. A number of the chartered banks also developed their own individual codes.

⁴⁴⁴ At the time the draft was released, it also indicated that adequacy would be measured with regard to the nature of data; the purpose and duration of the processing operation; the existence and scope of the general and sectoral data protection legislation in place; and any professional rules of Codes that applied.

representatives from federal and provincial governments.⁴⁴⁵ In 1991, they put forward a preliminary proposal to develop a national Model Privacy Code in order to establish common safeguards to protect the privacy of Canadian citizens and the confidentiality of personal information. The intent was to develop a national voluntary code which would become the cornerstone of a national voluntary compliance framework which would, in turn, guide and influence institutions to establish codes of standards particular to their own environments.

Christopher Berzins has suggested that the movement to develop the CSA Model Code was influenced by:

Two closely related considerations....The first was an attempt to respond to and assuage concerns repeatedly voiced in public opinion surveys about the increasing threats to privacy posed by the private sector's use of personal information. Flowing from this was the second consideration: voluntary privacy codes might pre-empt government regulation by demonstrating to politicians and the public alike that legislation to protect privacy in the private sector was unnecessary.⁴⁴⁶

Despite the development and release of the model code, there was still a move towards government regulation of the area. In January 1998, Industry Canada and the Department of Justice released a consultation paper entitled "The Protection of Personal Information: Building Canada's Information Economy and Society." Berzins argues that this consultation paper was carefully focussed in terms "most likely to mute business opposition."⁴⁴⁷ Certainly it is true that at the end of the consultation process, Perrin et al. claim that 5 requirements for a new private sector privacy legislation had become evident: (1) that the law must be based on the CSA standard; (2) that the same

⁴⁴⁵Stephanie Perrin & et al., *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto: Werwin, 2001) at xiii

⁴⁴⁶ Christopher Berzins, "Protecting Personal Information In Canada's Private Sector: The Price of Consensus Building" *Queen's LJ* 27 (2002) at 609

⁴⁴⁷ *Ibid.*

rules must hold for the entire country; (3) that the law must not set up barriers to trade nor be so permissive as to allow data havens or offshore rivals; (4) the Privacy Commissioner should be responsible for oversight; and (5) there was a need for public education and awareness.⁴⁴⁸

PIPEDA was the result of this consultation process and the drafting that happened after. *PIPEDA* received royal assent on 13 April 2000 and, as of 1 January 2004 is fully in force in Canada, applying to all personal information collected, used or disclosed in the course of commercial activities by all private sector organizations.⁴⁴⁹

Examining this evolution to see whether and how it accords with the governmentality approach previously discussed, a few things become quickly evident. First, it is noteworthy that the recognition of the need for the law appears to have come (at least in part) from concern about maintaining and facilitating Canada's international trading relationship. Arguably, this accords with a desire for security that extends beyond safety and into security in economic terms.

The commercial aspect of this law should not be overlooked either. The law was enacted under the federal trade and commerce power, and focusses primarily on commercial activities. Additionally, the business involvement in the development of the CSA Code, which forms the backbone of *PIPEDA*,⁴⁵⁰ creates a situation with an extremely unusual degree of commercial involvement in the drafting of the law. Again,

⁴⁴⁸ Stephanie Perrin & et al., *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto: Werwin, 2001) at xiv

⁴⁴⁹ S.4(1)(a) states that *PIPEDA* will not apply in provinces that have legislation in place that has been deemed substantially similar to *PIPEDA*. At present, Quebec, British Columbia and Alberta have such legislation in place, while Ontario has a Personal Health Information Act that has been deemed substantially similar. The text of this section focuses on the *PIPEDA* approach because, as was said during the Committee hearings on *PIPEDA*, *PIPEDA* is intended to form the "floor" for Canadian private sector privacy regulation – to set the minimum standard which all legislation and bodies must meet.

⁴⁵⁰ *PIPEDA* s.5(1) provides that, subject to sections 6 through 9, every organization shall comply with the principles set out in Schedule 1 of the Act. Schedule 1 is the CSA Model Code for the Protection of Personal Information.

re-viewing this in light of governmentality, I see clear evidence of a governance structure that is focussed on creating regulation that is welcomed and embraced; the public consultation process and the wholesale incorporation of a voluntary code developed in consultation with industry are strong moves towards a symbiotic regulatory relationship between government and commerce. Indeed, with the limited exceptions set out in the text, private sector organizations in Canada are essentially governed by the CSA Model Code – a code they themselves had a hand in drafting and which may be presumed therefore not to place an undue burden upon them – through the medium of *PIPEDA*.

Finally, to return to the discussion of “data protection” versus rights discourse, the CSA model code points strongly towards a data protection approach; regulating the collection, use and disclosure of personal information via a set of procedural principles clearly grounded in the data protection stream. The principles themselves, which are for the most part a clear (re)articulation of fair information principles, reinforce this. At their most basic, data protection instruments can be said to consist of a series of procedural directions which are intended, if adhered to, to protect privacy by controlling the collection, use and disclosure of personal information.

In addition, *PIPEDA*'s purpose clause must be considered. Section 3 of *PIPEDA* notes that:

The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of personal information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information for purposes that a reasonable person would consider appropriate in the circumstances.⁴⁵¹

⁴⁵¹ *PIPEDA* s. 3

Raab and Bennett have suggested that not only do data protection schemes presume the availability of information, thus implicitly authorizing its use, but “the political reality has often been that reaping the commercial and administrative benefits that stem from information technology and data-usage, rather than privacy protection, has prompted the legislation in the first instance.”⁴⁵² Certainly, that could be said to accord with this approach. The language of the purpose clause seems to take the fact and the necessity of the circulation and exchange of information as a presumptive starting point for protection. In addition, although this clause speaks of a “right of privacy”, that right is a limited and finite one. It is a right of privacy only with respect to one’s personal information, not a more general right of privacy inuring to the individual. Also, the already limited “right of privacy of individuals to their personal information” is then further balanced against “the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.” In combination with the presumption of data availability already noted, this is reminiscent of Clarke’s comment that fair information-based regimes effectively legitimize ‘dataveillance’ in return for limited procedural rights.⁴⁵³

Finally, it should be noted that *PIPEDA*’s “light flexible model”⁴⁵⁴ of enforcement also corresponds to the interests of businesses.

In the discussions of responsabilization, it was shown how the seeming dispersal of power that characterizes this mode of governance relies heavily upon individual responsibility. This shows in *PIPEDA*, particularly in its reliance on a complaint-based model of enforcement.⁴⁵⁵ Although s. 11(2) of *PIPEDA* does indicate that the Commissioner may initiate a complaint, she may only do so where there are reasonable

⁴⁵² Charles D Raab & Colin J Bennett, "Taking the Measure of Privacy: Can Data Protection Be Evaluated?" *International Review of Administrative Science* 62:4, 535 (1996) at 535

⁴⁵³ Roger Clarke, "Beyond OECD Guidelines: Privacy Protection for the 21st Century", online: <www.rogerclarke.com>.

⁴⁵⁴ Stephanie Perrin & al., *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto: Irwin, 2001) at 61.

⁴⁵⁵ *PIPEDA* s. 11(1)

grounds, I would suggest that this too may rely, at least to some degree, on individual agency; to date these Commissioner-initiated complaints have primarily been motivated by media coverage, arguably another form of individual agency and awareness raising. This expectation that individuals will be responsible for protecting their own data and will monitor their personal information and complain to the Commissioner is supported by the *PIPEDA* public education mandate⁴⁵⁶, about which more will be said in the next section.

Returning to the idea of responsabilization as a process of offloading responsibility from a centralized government model to a dispersed power structure, this approach is a very effective example of the process in action. Central government responsibility for personal information protection gets dispersed via the involvement of industry bodies in the legislative process and, ultimately, the incorporation of the industry-developed model code directly into the legislation. Further offloading takes place with the placing of responsibility for protection onto an administrative body, and within that body by placing the responsibility on a complaint-based process that is overseen by an ombuds-person rather than an order-making adjudicator. At each step then there is a clear movement towards a focus on individual agency and responsibility, with its attendant demonization and disdain for the “stupid user” individual who fails to exercise the requisite agency and protect themselves. As such, the government process(es) in relation to this absolutely support the positioning of this law as a piece of government action that supports and encourages a move towards an approach to power relations and individual agency that is intended to accord with socio-economic priorities and thus be embraced and adhered to rather than challenged.⁴⁵⁷

⁴⁵⁶ *PIPEDA* s. 24

⁴⁵⁷ Of course, the discourse of late has been moving towards a change in this model, with the Privacy Commissioner and others beginning to advocate for a move away from the ombuds-model and towards order-making powers (see for example: Jennifer Stoddart, Privacy Commissioner of Canada, “Second Appearance Before the House of Commons Standing Committee on Access to Information, Privacy and Ethics on Privacy and Social Media, 11 December 2012, online: <http://www.priv.gc.ca/parl/2012/parl_20121211_e.asp>. While this might be taken as contrary to my argument, I would argue that it is not. Rather, the move towards order-making powers can be seen as

ADMINISTRATIVE

When examining how administrative bodies mirror the responsabilization message, Garland looked at the rhetoric of welfare and employment insurance bodies. Fusco, looking at healthification, explored health and safety policies within a set environment. I would suggest that an analogous area of inquiry for these purposes would be administrative privacy protection bodies. In Canada, each province and territory has a privacy oversight body, sometimes a Commissioner, sometimes an Ombudsperson. These roles are created under the public sector privacy and access to information legislation that exists in each province and territory. In addition, *PIPEDA* sets up a federal Privacy Commissioner.

As discussed in the “government” section, the federal Privacy Commissioner acts as the overseer of federal public and private sector privacy laws. In Quebec, Alberta and British Columbia, the privacy commissioner of the individual province oversees the operation of the substantially similar private sector and public sector provincial legislation, while in Ontario the information and privacy commissioner is responsible for oversight of the substantially similar health information privacy legislation, as well as the public sector privacy legislation. In viewing these offices in terms of administrative action, however, I want to focus not on the oversight of government (provincial, territorial or federal) legislation, but rather on the policy messages that are disseminated by those bodies.

Looking first at the federal Privacy Commissioner, it is important to note that s.24 of *PIPEDA* explicitly creates a public education mandate for the Commissioner – she must foster public understanding; undertake and encourage public privacy research; work with organizations to develop *PIPEDA*-compliant policies and promote the purposes of

consistent with the original process of public consultation and attempts to match public expectations. As the public becomes more aware both of privacy and of invasions of it, there is greater public will towards a stronger enforcement power, a will that is being reflected in the call for a change in model.

PIPEDA. To date, the Privacy Commissioner of Canada has rarely explicitly addressed issues of reputation itself⁴⁵⁸, although the public Consultation conducted in summer 2010 focussed attention on personal information and reputation implications. While not speaking directly about reputation, however, the Commissioner has certainly made a number of applicable comments. As part of her public education mandate, the Commissioner develops guidelines and best practices recommendations in a number of areas. In recent guidelines for the release of personal information in online environments by administrative bodies, the Commissioner states that one of the factors that may outweigh public interest is the possibility that an individual to whom the information relates may be unfairly exposed to monetary, reputational or other harm as a result of a disclosure.⁴⁵⁹ In speeches in June and November 2009 the Commissioner and Assistant Commissioner again emphasized the relationship(s) between personal information regulation under *PIPEDA* and reputation.⁴⁶⁰ This reading accords with my interpretation in chapter 3 of this dissertation, that information posted online factors into the creation, maintenance and consultation of individual reputations.

The Commissioner does not just link *PIPEDA*, reputation and personal information in online spaces; in her guidance and policy documents as well as her speeches, she has emphasized the role of individual agency in this protection. The Fact Sheet on Social Network Sites and the Workplace recognizes the possibilities of reputation damage for

⁴⁵⁸ Though privacy and reputation is one section of a speech from 2009: Lisa Campbell and Daniel Caron "The Unique Challenges to Privacy Rights Caused by the Internet and Other Emergent Technologies" Internet Law Conference: The Second Wave: New Developments, Challenges and Strategies, 27-28 March 2008 online: <http://www.priv.gc.ca/speech/2008/sp-d_080327_lc_e.cfm>.

⁴⁵⁹ Office of the Privacy Commissioner of Canada: *Guidance Document: Electronic Disclosure of Personal Information in the Decisions of Administrative Tribunals*. Online: <http://www.priv.gc.ca/information/pub/gd_trib_201002_e.cfm>

⁴⁶⁰ Chantal Bernier "Protecting Personal Information in a Globalized Environment" Speech delivered at the 2009 Access and Privacy Conference, June 12, 2009. Online: <http://www.priv.gc.ca/speech/2009/sp-d_20090612_cb_e.cfm> and Chantal Bernier "Personal Data Protection Issues in a Globalized World" remarks delivered at 3d Conference of Francophonie Data Protection and Privacy Commissioners, 3 November 2009. Online: <http://www.priv.gc.ca/speech/2009/sp-d_20091103_cb_e.cfm>.

the organization and for individuals, and recommends that employers develop policies and procedures that employees will be made aware of and expected to conform to.⁴⁶¹ In her speeches, the Commissioner has emphasized both the responsibility of social network sites and the importance of privacy policies on those sites⁴⁶², as well as the damage suffered by individuals as a result of information available through these sites⁴⁶³ both professionally⁴⁶⁴ and personally⁴⁶⁵.

Similar messages can be found from the provincial commissioners. The Ontario Information and Privacy Commissioner (OIPC), for instance, has published public information materials including “When Online Gets Out of Line”⁴⁶⁶ and “Reference Check: Is Your Boss Watching? Privacy and Your Facebook Profile”. The latter states that:

If decisions about you are made based on information obtained from social networking websites, you may never know why you didn’t get the job, the interview or the promotion. At least for now, those decisions are likely being made by individuals for whom the “tell all” nature of web 2.0 tools, like social networking sites, still seem foreign, embarrassing, risky, or even seriously misguided in the business world. What you might see as fun and meaningless in a “Wall” post or photo could be interpreted as evidence of recklessness and lack of judgement by someone who doesn’t understand the context. Your activities, comments and views, even though you may have just been joking around with

⁴⁶¹ Office of the Privacy Commissioner of Canada *Fact Sheet: Privacy and Social Networking in the Workplace* (May 2009) online: <http://www.priv.gc.ca/fs-fi/02_05_d_41_sn_e.cfm>

⁴⁶² Jennifer Stoddart “Social Networking and the New Rules of the Road” speech delivered at the IAPP Privacy Summit (30 April 2009) online: <http://www.priv.gc.ca/speech/2009/sp-d_090430_e.cfm>

⁴⁶³ *Ibid*

⁴⁶⁴ Jennifer Stoddart “Privacy and the Social Networking Revolution” speech delivered to the Employees of the Bank of Canada (9 September 2008) online: <http://www.priv.gc.ca/speech/2008/sp-d_080909_e.cfm>

⁴⁶⁵ *Ibid*

⁴⁶⁶ Ann Cavoukian “When Online Gets Out of Line” Guidance Document: Information and Privacy Commissioner of Ontario online: http://www.ipc.on.ca/images/Resources/up-facebook_ipc.pdf Interestingly, this document is available through the Office of the Information and Privacy Commissioner of British Columbia as well.

your friends, all become part of an online resume that, inadvertently or not, becomes available to everyone.⁴⁶⁷

The OIPC document goes on to provide 5 tips for individuals to protect themselves from such instances: (1) thinking before uploading content; (2) being aware of what information can be found about you in an online search in order to address it; (3) removing or asking to have removed – where possible – any information you would not want to discuss in an interview or similar situation; (4) implementing whatever privacy controls are available; and (5) using SNS and online environments to build up a positive image of yourself.⁴⁶⁸

Note the way that these public education materials implicitly underscore the “stupid user” meme, primarily focussing on neither the problems with organizations⁴⁶⁹ nor the information practices of organizations but rather on how individuals should manage their personal information in order to protect themselves. The actual uses of the information are also left unexplored and primarily unregulated; instead they are implicitly affirmed as simply acceptable, something to be taken into account in decision-making. In essence, these policy recommendations and public education initiatives reflect a behaviour and approach that is consistent with an agenda of responsibilization; where the governmental legislation has dispersed responsibility to

⁴⁶⁷OIPC. "Reference Check: Is Your Boss Watching? Privacy and Your Facebook Profile" Information and Privacy Commissioner of Ontario.

⁴⁶⁸ *Ibid.*

⁴⁶⁹ That is to say, it would be just as easy for education and advocacy approaches to work with organizations to address the issues that create risks for users. First of all, any business model that is predicated on monetizing information provided by users must be viewed with skepticism. All five of the OIPC suggestions to users could be inverted and addressed with organizations instead. Organizations could be educated about and encouraged to understand self-presentation in online environments as not a mirror but rather as a social process that should not be relied upon as factual. SNSs could be encouraged to put in place stronger controls to prevent individual user information from being available or searchable to others. Default settings could be privacy-based rather than merely available but the responsibility of users to implement. Strong warnings could and should be issued about the dangers of using information from these spaces to base administrative decisions upon. These are all business model decisions, intended to benefit the SNS, and yet the responsibility for mitigating the negative effects of those decisions is being placed on the individual users rather than those who created the problem.

administrative bodies, these bodies are in turn warning both organizations and individuals about the danger and encouraging them to protect themselves.

COMMERCIAL

As the messages and expectations of governing bodies are transmitted through a number of different nodes of social, political and economic power, it is not sufficient to explore only the governmental/legislative and administrative approaches to reputation and personal information in online spaces. Just as Garland identified insurance and security/protection enterprises as key in reinforcing and regulating the responsabilization-meme within crime control, Fusco and Rose show how insurance companies and cleaners (for Fusco) and security (for Rose) also interact in healthification scenarios. In this section, I want to explore three related but separate approaches to capitalizing on issues of reputation and risk in online spaces, and show how each of them not only furthers the security agenda and offloads responsibility onto individual users but does so in ways that are not merely permitted but actually facilitated by the legislative and administrative regimes already discussed.

Let us first consider the purely “commercial” site – Reputation Defender. Reputation Defender was established in 2006 and now bills itself as “the world’s first comprehensive online reputation management and privacy company.”⁴⁷⁰ Reputation Defender has 4 suites of products. “My Reputation”, which conducts regular searches of information related to an individual or individual and spouse, provides them with regular reports of findings, and (for an additional fee) will engage in “reputation defence” of a reported problem. “My Child” offers similar services. In contrast to these reactive approaches, Reputation Defender also offers two proactive suites: “My Privacy” which offers regular scans too, while also identifying and removing personal information contained in publicly available pages, databases etc.; and “My Edge” which manipulates tags, and inundates sites with positive comments⁴⁷¹ to optimize reputation

⁴⁷⁰ <<http://www.reputationdefender.com/company>>

⁴⁷¹ <http://www.forbes.com/2007/05/24/google-search-reputation-cx-tech_ag_0525google.html>

formation and management in online spaces. The Better Business Bureau awards Reputation Defender an "A" rating, based on the length of time they've been operating and the number of complaints (11).⁴⁷² There are, of course, issues with the Reputation Defender model; the creation of a sphere where a good reputation is purchasable, a sphere where good reputation is available only to those who can afford one, the way it skews reputation by manipulating it, the questions of how effective the takedown requests and challenges are. But it is not the intent of this dissertation to critique the service. Rather, Reputation Defender is introduced here as an example of a commercial entity that is complicit in both the security/risk agenda perpetrated by governance and in supporting the "responsibilization" of the individual. By providing and advertising the service, Reputation Defender emphasizes the presumptive danger of reputation "in the wild". Further, the existence of the service also serves to subtly encourage (or perhaps even create) fear in the individual, fear not only of the very real issues revolving around reputation in online spaces but fear of what will happen should they, the individual, fail to adequately protect themselves. That is, if there is X chance of Y happening, then the existence of product Z will serve to inflate the perceived likelihood of Y happening while simultaneously imposing a "fault" upon s/he who has failed to avail themselves of product Z. Think, for example, of antivirus software.

Let us next consider a company which tried to position itself as the happy medium in the field – Rapleaf.⁴⁷³ Originally, Rapleaf catered to both businesses and individuals. The service provided to an individual was free and allowed any individual to register with her email address and upon signing in (having authenticated the email address) she was provided with a list of sites and information to which her email address is linked. For businesses, Rapleaf analyzes consumer/customer lists to assist with directed and personalized marketing and communications. Although Rapleaf's personal services are free, a fee is charged for the business analytics. Interestingly,

⁴⁷² <<http://www.bbb.org/greater-san-francisco/business-reviews/personal-services/reputationdefender-in-redwood-city-ca-204366>>

⁴⁷³ <<http://www.rapleaf.com/>>

perusal of the Terms of Use seems to suggest that the “free” service accorded to individuals may not have a monetary cost, but it does expose personal information collected through the reputation search to collection, use and disclosure by Rapleaf.⁴⁷⁴ In fact, Rapleaf has since ceased to provide the individual service, targeting only businesses and working as a data aggregator.⁴⁷⁵ Rapleaf thus becomes an interesting intermediary – and intermediate step – not only on the continuum of care/responsibilization but also in demonstrating the process towards responsabilization. First the company sets themselves up using concerns around reputation and online presence to encourage individuals to provide their personal information freely, then they focus on a business model that aggregates and commodifies that very information, selling it to commercial entities and in so doing actually increasing the very dangers that individuals were attempting to guard against.

At the far end of the spectrum from Reputation Defender are sites like The Whuffie Bank.⁴⁷⁶ “Whuffie” is the reputation-based capital in Cory Doctorow’s first novel, *Down and Out in the Magic Kingdom*.⁴⁷⁷ The term has since seen limited adoption, including being used later in a text about social capital⁴⁷⁸ and it is in this sense that The Whuffie Bank uses it. At present, The Whuffie Bank site is able, upon provision of a user name, to calculate a “whuffie” (score) for a twitter user and (a) identify other twitter users with similar whuffies as well as (b) contacts for the user who have higher whuffies. Whuffie is calculated by analyzing: endorsements (how many of your posts are

⁴⁷⁴ <http://www.rapleaf.com/terms_of_service>.

⁴⁷⁵ In fact, Rapleaf suffered a few negative press events, first when it appeared that the company was selling Facebook IDs commercially, and later when allegations surfaced that Rapleaf was working with its own subsidiaries to compile extremely detailed customer profiles.

⁴⁷⁶ <<http://www.thewhuffiebank.org/>>.

⁴⁷⁷ <http://craphound.com/down/?page_id=1625>. The novel takes place in a society where most economic needs are taken care of, and thus “whuffie” has become the organizing principle of caste and access. Whuffie may loosely be understood as a measurement of the reputation of the individual, a measurement that is dynamic and actively affected by how others view the actions of the individual. Doctorow’s system is visually represented and contains within it an audit trail, allowing one to see where and for what whuffie has been added or subtracted.

⁴⁷⁸ Tara Hunt, “The Whuffie Factor”, online: <<http://www.thewhuffiefactor.com/>>.

retweeted); influence (how many posts you retweet); connections (being endorsed by those with strong whuffies correspondingly raises your whuffie); and content (being retweeted based on your content rather than a link raises whuffie).⁴⁷⁹ Although the site is restricted currently to analysis of Twitter, the intent is to extend to analysis of any reputation-driven site, and presumably to cross-site analyses. A similar but more recent site is Klout⁴⁸⁰ which is able to analyze multiple SNSs – Twitter⁴⁸¹, Facebook,⁴⁸² LinkedIn⁴⁸³, Foursquare, and Google+⁴⁸⁴ – to derive its metrics. While Whuffie is one score, Klout provides metrics for reach (how many people you influence); amplification (the extent of your influence on them); and network (the influence of your network).⁴⁸⁵ Both sites allow users to actively navigate reputation, either “giving” or receiving whuffies from other users. Klout operates similarly, though users are able to give and receive K+, which impacts on score and entitles users to “perks”.

Klout has been criticized for its business model, which is based on matching businesses with high profile users through perks and other rewards.⁴⁸⁶ There appears to be no clear “corporate” interest at play in The Whuffie Bank. Whether a corporate interest or not, both sites have a relationship with responsabilization. By recognizing social capital as a “salary” and encouraging users to give whuffies/K+ to other users as well as to facilitate the growth of the analysis, individuals continue to have a role to play in both sites, and it is a role that encourages reliance on reputation even as it emphasizes that reputation is derived from any and all encounters.⁴⁸⁷

⁴⁷⁹ <<http://www.thewhuffiebank.org/static/faq>>.

⁴⁸⁰ <<http://klout.com/home>>

⁴⁸¹ <<http://www.twitter.com>>

⁴⁸² <<http://www.facebook.com>>

⁴⁸³ <<http://www.linkedin.com>>

⁴⁸⁴ <<https://plus.google.com/>>

⁴⁸⁵ <<http://klout.com/corp/kscore>>

⁴⁸⁶⁴⁸⁶ Stephen Williams “Chevy Gives Three Day Sonic Drives to Those With Big Klout” *Advertising Age* 28 (November 2011), online: <<http://adage.com/article/news/chevy-tests-sonics-high-klout-scores/231220/>>

⁴⁸⁷ Perhaps unintentionally, one of the other things The Whuffie Bank makes evident is the way that particular sites or communities may impact reputation differently. At present it measures only Twitter, but the site insists that a Facebook Whuffie measurement is in process, and it is my suspicion that the ratings

Harkening back to the Fusco notion of “technologies of normalization”⁴⁸⁸ it can be seen that each of these enterprises acts as a technology of normalization. The Whuffie Bank and Klout both encourage active user understanding of (and perhaps dependence upon) reputation; Rapleaf set out to allow users to verify and monitor their online presence, which in itself acts to exacerbate risk-consciousness and security fears, and the very fact of Reputation Defender is perhaps the most normalizing step of all. That is, just as anti-virus software has become *de rigueur* on computers as the need for constant vigilance has become more accepted, so too does the existence of such sites and technologies reinforce the idea that reputation is constantly at risk and in need of monitoring and defence. Reputation Defender and similar firms, by their approach and by their very presence, reinforce the idea not only that reputation risks are the responsibility of the individual to manage and guard against, but also that this responsibility is already the status quo. In this way, these various approaches create a kind of self-reinforcing feedback cycle, acting to encourage and reinforce the need for security while simultaneously emphasizing that constant vigilance and adherence to norms is the way to achieve that security. In this way, the very existence of such tools acts to normalize the need for them. The individual who fails to participate in this cycle has presumptively failed at her duty to protect and manage risk effectively. Thus, not only have the technologies been normalized, so too again has the individual responsibility been normalized and further ammunition provided for the disparagement of the stupid user who fails to be aware of and employ such tools.

INDIVIDUAL

In its purest sense, responsabilization refers to the creation not just of a sense of individual agency, but of individual responsibility – responsibility for meeting the aims and expectations of the larger social, political and economic bodies – the expectation

between Twitter and Facebook may well end up being quite different since users often employ the sites for different purposes or audiences.

⁴⁸⁸ Caroline Fusco, "Inscribing Healthification: Governance, Risk, Surveillance and the Subjects and Spaces of Fitness and Health." *Health and Place* 12 (2006) at 73

that individuals be active agents in shaping their own destinies and protecting themselves against risks via self-governance. The concern must be, however, with a process of responsabilization that has transcended governance and instead devolved to a focus solely on the 'stupid user'.

The Stupid User as the Responsibilized Individual

Understanding the process(es) of responsabilization is key to understanding the bulk of the rhetoric around reputation and personal information in online spaces. Fusco notes that:

Risk-avoidance behaviour, therefore, becomes viewed as a moral enterprise relating to issues of self-control, self-knowledge and self-improvement. It is a form of self-government, involving the acceptance and internalization of the objects of institutional government. Because the project of selfhood is never complete, but rather is continuing throughout the lifespan, so too the project of risk avoidance as a technology of the self is never ending, requiring eternal vigilance.⁴⁸⁹

This is an apt summation of the effects of responsabilization, but it is the idea of risk avoidance as a moral and ethical responsibility upon which I now want to focus. Rose has proposed what he terms an "ethopolitics" that "concerns itself with the self-techniques by which human beings should judge themselves and act upon themselves to make themselves better than they are."⁴⁹⁰ By invoking "ethics" in the term "ethopolitics", I again see the conflation of responsibility with morality; responsibility as moral delineator. When responsibility is put in these moral terms, it is interesting to consider both which populations are being Othered and what larger morality is being furthered by such judgements.

⁴⁸⁹ Caroline Fusco, "Inscribing Healthification: Governance, Risk, Surveillance and the Subjects and Spaces of Fitness and Health." *Health and Place* 12 (2006) at 73

⁴⁹⁰ Nikolas Rose, "The Politics of Life Itself" *Theory, Culture & Society* 18:6 (2001) at 18.

Rose divides the population into the affiliated – “those who are considered included: the individuals and families who have the financial, educational and moral means to pass in their role as active citizens in moral communities”⁴⁹¹ – and the marginalized, and identifies the marginalized as including “the underclass, the excluded, the marginal.”⁴⁹² Fusco makes an interesting point that “it is ironic that members of the working class have historically been represented as the archetypal uncontrolled body in public health discourse, because it has been working classes, immigrant or slave groups that have served the bourgeois by keeping spaces clean.”⁴⁹³ Admittedly, the digital-divide literature would support the idea that marginalized populations are still excluded from full participation in online spaces, however it is not access to online spaces that is at issue here, but participation in them and the reputation that is derived from (and based on) that participation. There is a compelling analogy here, to those working classes keeping the spaces clean whilst themselves being considered “unclean” within public health discourse. That is, perhaps those who participate “indiscriminately” in online spaces are the modern equivalent of that underclass; after all, the information they provide is what makes advertisers support social networks, and the cost-free access to social networks is supported, for the most part, by advertising. In this way, just as “they” make it possible for “us” to have clean healthy spaces despite our demonization of them, perhaps “they” who are demonized for their mode of participation and free sharing of information in online spaces are also the ones who make it possible for “us” to have access to those spaces? ⁴⁹⁴

⁴⁹¹ Nikolas Rose, "The Death of the Social? Re-Figuring the Territory of Government" *Economy and Society* 25:3 (1996) at 340.

⁴⁹² *Ibid.*

⁴⁹³ Caroline Fusco, "Inscribing Healthification: Governance, Risk, Surveillance and the Subjects and Spaces of Fitness and Health." *Health and Place* 12 (2006) at 71.

⁴⁹⁴ Of course, I am not claiming that SNSs are populated by information provided by the same working classes, immigrants and slave populations identified by Fusco. That said, most SNSs at least in their early incarnations have been populated by Other populations (Friendster); youth (MySpace) and students (Facebook). It might be suggested, at least on a superficial level, that these populations are similarly likely to lack economic power and/or the status to prevent themselves and their products/content from being exploited for the benefit of the bourgeoisie.

In such a situation, who are the marginal? It is not merely a case of numerical superiority; groups are marginalized by power structures, not by numbers. Deleuze reminds us that “the difference between minorities and majorities isn’t their size. A minority may be bigger than a majority. What defines the majority is a model you have to conform to: the average European adult male city dweller, for example...a minority on the other hand, has no model....”⁴⁹⁵ I am not as certain that a minority has no model – indeed, discussions about community norms and identity performance in Chapter 3 certainly suggest that there are models out there – but I do think it is clear that a minority lacks a model that is coercive outside their own community.

Where affiliation is defined by inclusion and participation, “to remain affiliated, one must enterprise one’s life through active choice, within authoritative terms and limits that have become integrated within all the practices of everyday life, sustained by a heterogeneous array of civilized images and devices for lifestyle promotion.”⁴⁹⁶ Where adherence to the expectations and norms of the majority is the defining feature in affiliation, this means that the means to move from “marginalized” to “affiliated” is both clear and restrictive. That is, in order to be affiliated, you must assimilate. The marginalized “must show themselves capable of calculated action and choice, they must shape their lives according to a moral code of individual responsibility and community obligation.”⁴⁹⁷

This process of using moral judgements to maintain a feeling of security is not unique to questions of reputation or even of online participation, of course. As an example, let us consider the moralities at play when a sexual assault is reported and prosecuted. All too often, processes focus on the actions and credibility of the person who was victimized. Questions arise: What was she wearing? What neighbourhood was she in?

⁴⁹⁵ Gilles Deleuze, *Negotiations*, 1972-1990, Translated by Martin Joughin (1990) at 173.

⁴⁹⁶ Nikolas Rose, "The Death of the Social? Re-Figuring the Territory of Government" *Economy and Society* 25:3 (1996) at 340.

⁴⁹⁷ *Ibid.*

Was she drinking? The believability of the claimant becomes a question of morality, not creditability.

In *The Story of Jane Doe*, discussing previous rapes committed by the Balcony Rapist, the author ascribes the following voice/thoughts to the police officer (Bill Cameron) who first recognized the serial nature of the crimes:

The first incident was six months ago and she's mad as hell at us because the cop who caught the call at 51 didn't believe her, didn't find cause to file a charge and even then suspected it was her boyfriend who did it and arrested him! According to the report, she had sex aids, handcuffs and ropes all over her bedroom. Jesus. The second vic's apartment superintendent said she was a troublemaker and her boyfriend thinks she's nuts and there's something about potato chips on the bed⁴⁹⁸ that sinks us, but that happens much later. The third girl lives in the same apartment building as the second, and 51 files that one but doesn't connect the two...⁴⁹⁹

Look at the moral judgements encapsulated here; sexual activity and/or "kink" made one woman presumptively un-rapeable, while another was put into the same category because she was "difficult" rather than conforming to expectations of femininity.

Sherene Razack suggests that for a woman to succeed in sexual assault proceedings, "she must, in effect, establish her virtue – for the legitimacy of her claim to the court's protection is based on belonging to a group whose virtue must be protected."⁵⁰⁰

Stepping outside the bounds of belonging – of meeting the expectations of the mainstream – is judged a moral failure and protections may not be extended or may be weakened as a result.

⁴⁹⁸ The fact that a bowl of potato chips on the bed was not spilled during the assault was taken as an indicator that no assault had taken place.

⁴⁹⁹ Jane Doe, *The Story of Jane Doe: a book about rape* (Canada: Random House, 2003) at 18

⁵⁰⁰ Sherene Razack, *Looking White People in the Eye: Gender, Race and Culture in Courtrooms and Classrooms* (Toronto: U of Toronto Press, 1998) at 143

In proposing this analogy, I in no way seek to diminish the trauma of sexual assault or to claim that a violation of informational self-determination is equivalent to sexual assault. I do, however, want to suggest that there is a lesson to be learned from sexual assault activism and jurisprudence – that when a moral judgement is layered over a legal/factual determination, the focus of the determination shifts – no longer is the determination based on what is, but rather becomes focussed on whether the complainant is recognized as deserving of having the social and legal apparatuses intervene on her behalf.

Identifying the norms that come to ground the governance programmes (for crime control, in his case), Garland writes that “the programmes and ideas that are thus selected are those that fit with the field’s dominant structures and the specific cultures they support. They are the ones that mesh with the most powerful institution, allocate blame in popular ways, and empower groups that currently command authority, esteem and resources.”⁵⁰¹ Similarly, then, the “appropriate” way(s) for individuals to act are (or become) those that are in accordance with the expectations of the political, administrative and commercial entities who are involved in the governance project.

At this stage, then, it is imperative to ask if this is truly the right or even the desired approach. Should individuals have to “earn” the right to protection? Speaking about the role of myths and stereotypes about sexual assault, Adelyn Bowland argues that rather than conform in order to be considered deserving of protection, “we must be free to choose many partners or no partner, conventional sexuality or practices considered “deviant” by mainstream society. As long as we are not protected from sexual assault by virtue of our ‘unchastity’, we will continue to be held hostage in the

⁵⁰¹ David Garland, *The Culture of Control: Crime and Social Order in Contemporary Society* (Chicago: University of Chicago Press, 2001) at 26

old ways, concerned about what people think, even more fearful of our own sexual aspirations.”⁵⁰²

To explore Bowland’s point in this context, let’s revisit the “stupid users” from the beginning of this chapter.

Staples’ customers for instance; when they are critiqued for failing to ensure that their data was removed from the devices before they returned them, a clear message is sent that an organization bears no responsibility for meeting their legal obligations. Rather, it is incumbent on the individual to protect themselves in advance and at all times. Failure to protect themselves by erasing the data is positioned as a personal failure and the individual considered blameworthy and thus undeserving of protection. That’s certainly what the comments on the news story would suggest.

Natalie Blanchard too suffers from a perceived failure to act appropriately – to protect herself – that makes her undeserving of the protection of law (or even the sympathy of the public). Despite the fact that she was following medical advice, that she behaved in a transparent way (notifying her insurance company, posting photos etc), and that depression and other mental illnesses are not easily or visually diagnosable, her behaviour was still considered blameworthy both by Manulife and (seemingly) by outsiders looking at the situation.

Finally, Corporal Brown. Despite Trudeau’s famous statement in 1969, that “there is no place for the state in the bedrooms of the nation,” ⁵⁰³ Corporal Brown is not considered blameless in this situation either, despite the fact that his activities took place during off-work hours. Rather, the publicness of his behaviour is being used against him

⁵⁰² Adelyn Bowland, "Sexual Assault Trials and the Protection of Bad Girls" in Julian V Roberts & Renate M Mohr eds., *Confronting Sexual Assault: A Decade of Legal and Social Change* (Toronto: University of Toronto Press, 1994) at 263.

⁵⁰³ <<http://www.cbc.ca/archives/categories/politics/rights-freedoms/trudeaus-omnibus-bill-challenging-canadian-taboos/theres-no-place-for-the-state-in-the-bedrooms-of-the-nation.html>>.

(whether it is the erroneous identification of him as part of the photo shoot or the larger question of his participation on an online BDSM site). It is clear from the articles, especially the comments by Mike Webster, that Corporal Brown's activities are being used to call not only his behaviour as an employee into question but in fact to call him as a moral person into question. Again, by virtue of public behaviour, Brown is considered disentitled to protection against these invasions, either due to the nature of the acts with which he's associated (erroneously) or, among those who defend his right to freedom of sexuality, for the public act of having a profile on the site which is read as indicative of a lack of judgement.

Examining reputation systems, both formal and informal, in Part I, I showed how dominant norms exert a regulating force that serves to uphold and reinforce themselves whilst punishing those who deviate from them. That reinforcement is evident in each of these situations; failure to internalize norms and behave as expected at all times results in each case in judgement against the individual. This is the process of responsabilization in action; it ultimately acts not only to place responsibility on the individual to conform to those norms, but also to bolster the norms themselves.

In this chapter, I revealed the various avenues through which those norms are reinforced. In terms of reputation, that means government and legislative models that are complaint-driven; public education messages that emphasize the risks of these behaviours; and commercial enterprises built on the need for vigilant monitoring of information. All of these are, ultimately, self-fulfilling and self-supporting. The culture of risk upon which they are founded, and the individual agency and action they demand, create an impetus not only to act, but to think in ways that accord with the desires of the governing body(s). Indeed, with so many sites online dependent on personal information and reputation to facilitate user interaction and revenue generation, an odd balance is struck, where the information models of these spaces remain unquestioned and the actions of those who use them are problematized instead.

Conclusion

Discussing sexual assault and the desired transformation of the traditional model of sexual assault law and policing, Bowland was clear that true transformation cannot require particular behaviours or attitudes in order to extend protection. In this context, that means that individuals must be able to share information and select and perform identities informed by the context(s) in which they find themselves without fear of irrelevant information and inferences drawn from it and from mainstream myths and assumptions being used against them.

This chapter's project of unpacking both the stupid user meme and the process of responsabilization itself is the final step in the project of the under-labourer.

Just as the importance of social processes and context was made explicit in Part I, Part II makes it clear that in order to regulate reputation effectively and to appropriately address all its attendant issues and implications, a full understanding of context will be necessary; not just the online context, but the way(s) in which our investments and assumptions, socially, politically and economically, are implicated.

Garland recognizes that

Structures, and above all structural changes, are emergent properties that result from the recurring, reiterative actions of the actors who occupy the social space in question. The consciousness of these actors – the categories and styles of reasoning with which they think and the values and sensibilities that guide their choices – is therefore a key element in the kind of production of change and the reproduction of routine...⁵⁰⁴

In the realm of reputation, as long as the focus remains on demonizing the “stupid user” as undeserving of protection – indeed, as somehow “asking for” any negative effects

⁵⁰⁴ David Garland, *The Culture of Control: Crime and Social Order in Contemporary Society* (Chicago: University of Chicago Press, 2001) at 24.

s/he suffers – the underlying systems that permit those negative effects not only remain in place but, at least arguably, are fortified as individuals are required to conform to their needs, demands and expectations.

Garland also commented that “to the extent that the government succeeds in organizing, augmenting and directing the social control capacities of citizens, corporations and communities, it simultaneously extends its governmental reach and transforms its mode of exerting control.”⁵⁰⁵

This final chapter examined the process of responsabilization and the attendant expectation that the individual manage her own reputation. As part of this analysis, various approaches were re-viewed, from individual education through to commercial organizations that promise (for a fee) to “protect” and “correct” one’s reputation. Responsibilization is, ultimately, a process where government avoids or offloads the obligation to protect citizens by making self-protection a moral obligation. Applying this idea to reputation showed that existing facets of reputation discussion and regulation ultimately act to reinforce and normalize individual responsibility for risk management.

The examination here shows directed governance that privileges business interests and data protection and demonizes those who step outside the expected parameters. That cannot be an appropriate or sufficient way to regulate reputation.

Having fully explored how reputation is constructed and functions; how such information is being used and the effects that may result from such use; current regulation in law; and existing governance approaches, it is clear that something new is needed. A new thinking about reputation that takes into account all of its complexities and one that situates responsibility where it belongs in order to best regulate the area.

⁵⁰⁵ David Garland, *The Culture of Control: Crime and Social Order in Contemporary Society* (Chicago: University of Chicago Press, 2001) at 24

After all, we are all “stupid users” unless and until we can reshape the process that constructs us as such.

CONCLUSION:
Towards a Framework for Reputational Governance

Mandate

At the outset of this project, I took on the mantle of the under-laborer; s/he who is engaged “in clearing the ground a little, and removing some of the rubbish that lies in the way to knowledge.”⁵⁰⁶ This project, then, positions itself as a prerequisite, an important and necessary precursor to dealing with the issue of the appropriate regulation of reputation.

Julie Cohen argues that “meaningful information law and information policy requires a deep and fundamental rethinking of the most basic assumptions on which they are founded.”⁵⁰⁷ As part of this rethinking she encourages an awareness of the important intersections of culture and information, as well as the everyday relationships in which information is implicated.

Any reform to the law must not interfere with these important ideas, and must have at its heart the well-being of the individuals.

The ultimate goal is to develop knowledge, and the under-labourer takes on the responsibility of clearing the way towards that knowledge. Locke spoke of clearing away rubbish, but that task is not as simple as it sounds; in order to clear away rubbish, one must first identify what is important and what is rubbish. It is for this reason that Part I of the project set out to develop a deep understanding of the subject. Accordingly, in the first part, the idea of reputation was established and interrogated.

⁵⁰⁶ John Locke, “An Epistle to the Reader” *An Essay Concerning Human Understanding*, 9, ed. P. Nidditch, (Oxford, Clarendon Press, 1975).

⁵⁰⁷ Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press, 2012) at 267.

In chapter 1, the notion of reputation was introduced and subjected to rigorous scrutiny – what it is, how it is derived, what its function is – in order to understand the full complexity of the subject matter and to understand it as a social artefact.

Chapters 2 and 3 engaged with the intersections of culture and information and the effects of those intersections on the derivation and meaning of reputation. This was done in two ways: first, by examining formal reputation systems and the way(s) their users are implicated in reputation; and then by looking at the information and reputation assessments that shape our performance of identity on and offline and linking those same forces back to reputation.

Having explored the intricacies of reputation and shown how identity is negotiated and re-negotiated within social interaction, chapter 4 moved to inquire into whether reputation needed to be regulated; that is, whether harm can result from reputation and, if so, what that harm might encompass.

With the subject – reputation – firmly grounded in Part I, I was then able to parse and examine the existing systems around reputation more accurately in Part II.

Thus, chapter 5 reviewed the existing legal methods through which reputation injuries might currently be addressed or redressed, and concluded that none of them were sufficient to address the full complexity of reputation as set out in Part I.

Finally, chapter 6 looked at the underlying expectations that shape attitudes towards reputation, demonstrating a move towards governance via individual responsibility. Examining and challenging the assumptions upon which this move depended led to a recognition that in order to regulate reputation effectively and to appropriately address all the attendant issues a holistic view will be necessary; not just in the online context, but in the way(s) in which our investments and assumptions, socially, politically and economically, are implicated.

At the end of this process of re-view, it can be said that the rubbish that risked obscuring the path to knowledge has been cleared and the path is ready to be negotiated.

Deconstructing Norms

Having established the fact of responsibilization and then challenged its fundamental precept that an individual should or does bear the sole responsibility for reputation, this process of re-thinking shows, as a start, that neoliberal laws and policies that focus on the individual have the effect of pulling reputation out of its social context. The social context must be recognized as integral to both understanding and ultimately regulating reputation.

Merely focussing on the social context alone, however, is not sufficient. The discussion of norm creation and negotiation is not just about recognizing the role of norms in reputation; rather, I have also striven to show the way(s) in which particular political, economic and ideological investments and interests may act to create, shape and encourage particular norms.

Thus, it is important not only to understand the social context, but also to understand the process of (dominant) norm creation and the way(s) in which those norms may have particular imperatives embedded within them. This recognition is important; it cannot therefore be sufficient merely to incorporate the social, it is also necessary to ensure that those interests that are extraneous to social negotiation are not mistakenly understood as social and thus (super) imposed on social actors.

Distinguishing the Existing Approaches

We have, then, a range of laws and legal approaches that deal with some aspects of reputation, but none that address reputation as fulsomely or holistically as is required.

In her discussion of the intersection of racism and defamation, Sutherland expresses concern that the availability of defamation as a response may have the effect of shutting

down public discourse about the issue.⁵⁰⁸ That is, while there is a positive impact in being able to name racism as defamation, at the same time governments and policy makers are less likely to identify it as an urgent issue due to perceptions that there already exists a legal remedy. In considering appropriate legal response(s) to reputational harm, this is a key critique. As Ann Bartow comments:

When it appears that self-help options are available, momentum for official intervention can dissipate. Government actors may decline to assist online harassment victims because the more affluent ones can theoretically purchase assistance from Reputation Defender or similar services. They might not see a need to step in and have the government provide assistance that could readily be purchased, at least by those who can afford it. The role of “Internet Editor” in the context of defamation and harassment has been ceded to private companies like Reputation Defender, since neither norm entrepreneurs nor the legal system have effectively taken it on. Meanwhile, reputation defense services have strong incentives to derail public efforts to address the problems that they purport to solve for a price.⁵⁰⁹

It is for this reason that chapter 5 sought not only to identify the existing avenues of regulation but to show how each of them was inadequate, insufficient, or (in the case of extralegal regulation) perpetuating particular political and economic agendas that may skew the focus rather than solve the issue(s).

Valuing Reputation

Similar to the notion of “privacy”, reputation may be understood as both an individual and a community value. This is perhaps best exemplified by Lord Nicholls of Birkenhead’s statement in *Reynolds v. Times Newspapers Ltd.*⁵¹⁰:

⁵⁰⁸ Kate Sutherland, “The Impact of the Tort of Defamation on Public Discourse About Racism” *Critical Torts*, edited by Rakhi Ruparelia, Sandra Rogers and Louise Belanger-Hardy (2009)135, at 135.

⁵⁰⁹ Ann Bartow, “Internet Defamation as Profit Center: The Monetization of Online Harassment” (2009) 32:2 *Harvard Journal of Law and Gender* at 140

⁵¹⁰ [1994] 4 All E.R. 609 at 622 (H.L.)

Reputation is an integral and important part of the dignity of the individual. It also forms the basis of many decisions in a democratic society which are fundamental to its well-being; whom to employ or work for, whom to promote, whom to do business with or to vote for. Once besmirched by an unfounded allegation in a national newspaper, a reputation can be damaged forever, especially if there is no opportunity to vindicate one's reputation. When this happens, society as well as the individual is the loser. For it should not be supposed that protection of reputation is a matter of importance only to the affected individual and his family. Protection of reputation is conducive to the public good....Consistently with these considerations; human rights conventions recognize that freedom of expression is not an absolute right. Its exercise may be subject to such restrictions as are prescribed by law and are necessary in a democratic society for the protection of the reputations of others.

Interestingly, the germinal Canadian case on defamation appears silent on the community aspect of the importance of reputation, with Cory, J. focusing instead on the individual with statements such as “[a] good reputation is closely related to the innate worthiness and dignity of the individual. It is an attribute that must, just as much as freedom of expression, be protected by society’s laws”⁵¹¹ and that “the protection of a good reputation is imperative in a democratic society.”⁵¹² Nevertheless, these statements make it clear that reputation is a key right; one that has important social value.

Especially given this recognition of social value, it is troubling that existing legal remedies do not appear to fully or effectively address the issue. As Citron realizes, “traditional criminal and tort remedies play an important role...but they cannot reach all of the harm experienced by individuals, groups and society when defendants interfere with individual’s right to equal treatment.”⁵¹³

⁵¹¹ *Hill v. Church of Scientology of Toronto* (1995), 184 N.R. 1 at 60 (S.C.C.)

⁵¹² *Hill v. Church of Scientology of Toronto* (1995), 184 N.R. 1 at 60 (S.C.C.) at 65.

⁵¹³ Danielle Keats Citron, "Law's Expressive Value in Combating Cyber-Gender Harassment" (2009) 108:3 *Michigan Law Review*, at 405

Writing about healthification and locker rooms, Fusco identified an interesting tripartite hierarchy of regulation with laws as the first level; rules, policies and norms as a second level; and individual governance and surveillance underneath it all.⁵¹⁴ In the earlier analysis of reputation, both the second and third levels were evident, but the laws themselves were still lacking an appropriate approach. Nor can, or should, there be any suggestion that proceeding without law can be effective; as has been seen, reputations are influenced on many levels, may act to reinforce existing inequalities, serve as gatekeepers for access to cultural participation, information and services, and may ultimately have the effect of widening those inequalities. These are important areas, ones that need attention.

Towards a Framework for Reputational Governance

Established Points:

This project of re-viewing reputation has established the following:

1. that individuals are affected by and use reputation in multiple ways⁵¹⁵;
2. that reputation is not chosen or self-governed, but rather is the result of an ongoing and dynamic web of social and community assessment and engagement⁵¹⁶;
3. that reputation is intimately linked with the performance of duties and obligations by individuals; both as a result of them, and by influencing the future performance thereof⁵¹⁷;
4. that reputation may, therefore, impact on the ability of an individual to define for themselves the life they desire;⁵¹⁸

⁵¹⁴ Caroline Fusco, "Inscribing Healthification: Governance, Risk, Surveillance and the Subjects and Spaces of Fitness and Health." *Health and Place* 12 (2006) at 73.

⁵¹⁵ Chapters 1-4

⁵¹⁶ Chapter 1

⁵¹⁷ Chapters 1-4

⁵¹⁸ Chapter 4

5. that reputation may hinder or act as a barrier to the achievement by an individual of this life⁵¹⁹; and
6. that it should not be solely the duty or responsibility of the individual to protect and monitor her information to prevent reputation damage.⁵²⁰

What kind of reputation framework could be built that would address these social requirements?

The Need for Law:

First, to answer the question of whether a law or legal approach is necessary for the effective governance of reputation, I contend that it absolutely is. Not because people are inherently bad or fraudulent, not because reputations are manipulated or people defamed maliciously or frequently, but because, at its root, law is about something beyond the regulation of behaviour. Citron discusses this role, writing that:

[L]aw has an important expressive character beyond its coercive one. Law creates a public set of meanings and shared understandings between the state and the public. It clarifies and draws attention to the behaviour it prohibits. Law's expressed meaning serves mutually reinforcing purposes. Law sees educates the public about what is socially harmful. This legitimates harms, allowing the harmed party to see herself as harmed. It signals appropriate behaviour. In drawing attention to socially appropriate behaviour, law permits individuals to take these social meanings into account when deciding on their actions. Because law creates and shapes social mores, it has an important cultural impact that differs from its more coercive effects.⁵²¹

Giddens concurs, emphasizing the role of law in reinforcing a shared reality of community and community standards.⁵²² Understood in this transformative, rather

⁵¹⁹ Chapter 4

⁵²⁰ Chapter 5

⁵²¹ Danielle Keats. Citron, "Law's Expressive Value in Combating Cyber-Gender Harassment" *Michigan Law Review* 108:3 (2009) at 407.

⁵²² Anthony Giddens, *Modernity and Self-Identity* (Stanford: Stanford University Press, 1991) at 36

than simply coercive, role it is clear that a legal standard must be set to deal with reputation, especially as reputation continues to ascend in importance.

Not only is it important that a legal standard be set, it is important that it be set as soon as possible. The patchwork of approaches currently employed are not only demonstrably insufficient and ineffective, but their continuing existence, with nothing more, may have the effect of discouraging government or policy approaches to reputation. Having analyzed reputation and demonstrated its inherent subjectivity and the way it functions to reinforce existing inequalities, it becomes evident that an effective approach must be envisioned and implemented as soon as possible before these attitudes and problematic inequalities become so entrenched and normalized that challenge or change is unthinkable.⁵²³

What, then, should a framework intended to deal not only with reputation, but to transform our understanding of it and protect against fostering inequality and discrimination look like? Having reviewed the various forms of law that currently could be applied and demonstrated how each fails to be truly effective, it seems to me that in order to be effective an entirely new approach is needed. It is not, and cannot be, sufficient to attempt to tweak or expand any of the existing approaches in order to make them better address reputation.

CONCLUSION 1: There is a need for a formal legal mode of regulation

Aspirational Approach

The 2000 La Forest-authored review of the *Canadian Human Rights Act* (re)examined the role of the Human Rights Commission and of human rights legislation. It was the conclusion of the panel that the Act should be understood as something more than an individual remedy; rather, that it had a transformative function, signalling (both

⁵²³ Danielle K. Citron, "Law's Expressive Value in Combating Cyber-Gender Harassment" *Michigan Law Review* 108:3 (2009) at 409

through its provisions and through the education mandate contained within the Act) agreement on basic standards of rights entitlements. For the panel, the overriding commitment of the Act was towards equality, and they dismissed the notion that groups in need of rights protection were “special needs” groups, arguing instead that the Act:

...should reflect the idea that everyone should have the same right to participate in the matters covered by the Act. This involves adopting the notion of “substantive equality” which requires an acceptance of the fact that everyone is different and that positive measures may be needed to ensure that some individuals may participate as fully as others. These equalization measures should not be looked on as “special” measures but rather as simply what it takes to recognize the right of everyone to participate as fully as they can in work and services. The Act should refer to the goal of full participation.⁵²⁴

In this conclusion, I believe we see the intersection of many of the threads that have emerged in the foregoing examination of reputation and of appropriate legal responses to it.

First, we see the recognition that law may be aspirational. That is, that it need not (and does not) merely grant individual remedies but rather functions as a statement about the chosen norms and values of a particular jurisdiction or community. I have discussed previously the role of law in sending such a message, and here we see validation of that role, albeit attached specifically to human rights legislation.

Reputation must be positioned as an important public issue. Recall that in parsing some of the existing legislative approaches – the Criminal Code provision on defamatory libel specifically – I suggested that they were inadequate in part because of the failure to understand reputation as reputation was not yet understood as an important public issue.

⁵²⁴ LaForest, et al. "Promoting Equality: A New Vision: Report of the Canadian Human Rights Act Review Panel." (2000) at 8.

Potentially, creating a framework for dealing with reputation might also mirror the transformative impact of human rights legislation; that is, the creation of the framework comes to function as an education tool in itself to assist others in understanding the important role played by reputation and the necessity of governing it appropriately.

In addition, the recognition that those needing protection do not have “special needs” but rather must be assisted in attaining an equal status is key. There exist already legal remedies for blatant violations of trust and law; charges of fraud, theft, breach of trust and the like. There are also civil avenues available to those who wish individual redress for such a violation. As I have demonstrated in chapters 2 and 3, what is most problematic in reputation is also most difficult to address; the ways in which mainstream assumptions and expectations are embedded and enforced via reputation. Lessons can be learned from the human rights process, ensuring that reputation does not become a way of persecuting or punishing those who do not conform or choose not to conform to social conventions.

CONCLUSION 2: The law should have an aspirational intent. Simple redress is not sufficient

Scope of Law

In seeking to envision how law might best deal with reputation, it is important to first examine the role of law holistically and consider how it might best approach the issue.

Given that so much of the emphasis on reputation (and especially its role in limiting or granting access) relates to online spaces, we must first consider whether a reputation law initiative should focus exclusively on those spaces or be conceived as a law of more general application.

Certainly earlier analysis has demonstrated that there is a tension. Although reputation can and does exist in offline as well as online spaces, and the reputations that are derived in online spaces are inherently influenced (both in performance and in review) by offline expectations and norms, at the same time online spaces have greatly facilitated the fragmentation of publics and thus created an attendant challenge to any homogenous notion of community standards.

Discussing cyber-gender-harassment, Danielle Citron conclusively rejects the idea that “the net has its own norms”, analogizing this belief to earlier public/private distinctions that, far from protecting the vulnerable, acted to perpetuate abuses and erase the voices of those so victimized.⁵²⁵ This analogy has resonance, especially as Human-Computer Interaction analyses are increasingly recognizing the socio-technical interrelationships between online and offline spaces. Accordingly, any law designed to address reputation issues should be envisioned as applying to reputation in its entirety – not as restricted to one technology or to contemporary issues, but as a law of general application, flexible enough to encompass new technologies and evolving understandings of reputation.

CONCLUSION 3: Regulation must be focussed on reputation, both online or offline rather than on technology or technologically-mediated or applied reputation

Focus

As discussed in chapter 6, the current approach to regulation (such as it is) tends to focus on individual responsibility. In so doing, it obscures the roles and interests of other stakeholders: state governance investments; commercial interests; and other norms and assumptions that are built into the architectures of control and into the code itself, socially and online.

⁵²⁵ Danielle K. Citron, "Law's Expressive Value in Combating Cyber-Gender Harassment" *Michigan Law Review* 108:3 (2009) at 401

Accordingly, it is important that any regulatory approach to reputation understand the full scope of powers and interests at play and address them accordingly. This cannot be accomplished via individual responsabilization.

CONCLUSION 4: It must relate to the derivation and use of reputation by organizations rather than placing responsibility for protection and management on the individual

Identifiability

Linked to the suggestion of an online-specific approach are theories that focus on identification and identifiability of parties. Especially in areas such as cyber-bullying, cyber-harassment and cyber-stalking, there is much discussion of the way(s) in which anonymity may enhance the abuser's power or even encourage behaviour that would not be modelled were it visibly attached to an offline (or even just a fixed) identity. Grimmelmann, recognizing that identifiability often translates into accountability⁵²⁶, posits⁵²⁷ a system where complainants could trade their right to future legal remedies for reputation harm in exchange for learning the name of the person (or, presumably, persons) responsible for a particular harmful posting or comment.⁵²⁸ In some ways, this might be thought of as the polar opposite of a SLAPP⁵²⁹; rather than a lawsuit intended to silence, it would be a short procedure intended to provide accountability without invoking legal punishment(s). Looking at anonymity from another angle, Solove proposes that "people should be able to sue without having their real names appear in the record. This would allow people to seek a remedy for the spread of

⁵²⁶ James Grimmelmann, "The Unmasking Option" *Denver University Law Review Online*. (Jan. 2010) 23, online:

<http://works.bepress.com/james_grimmelmann/29> at 26.

⁵²⁷ Although he later dismantles the proposal, showing that it wouldn't work.

⁵²⁸ James Grimmelmann, "The Unmasking Option" *Denver University Law Review Online*. (Jan. 2010) 23, online:

<http://works.bepress.com/james_grimmelmann/29> at 24

⁵²⁹ SLAPP: Strategic Lawsuit Against Public Participation, online: <<http://www.casp.net/>>

information about them without having to increase the exposure of the information.”⁵³⁰ Accountability must be, however, a two way street, and any legal approach that intends to deal effectively with reputation must balance these issues appropriately.

On 27 September 2012, the Supreme Court of Canada released its decision in the *A.B. v. Bragg Communications Inc.* appeal. That case deals with a young woman who wished to have the identity of the persons(s) who created a false Facebook profile about her revealed in order to bring a defamation claim against them. At issue in this proceeding was her desire to proceed with the claim while protecting her own identity. Writing for the Court, Justice Abella found that:

If we value the right of children to protect themselves from bullying, cyber or otherwise, if common sense and the evidence persuade us that young victims of sexualized bullying are particularly vulnerable to the harms of revictimization upon publication, and if we accept that the right to protection will disappear for most children without the further protection of anonymity, we are compellingly drawn in this case to allowing A.B.’s anonymous legal pursuit of the identity of her cyberbully.⁵³¹

In its finding that the plaintiff could proceed while protecting her identity, the court invoked its previous jurisprudence on sexual assault complainants and anonymity, holding that the risks to bullied children and the administration of justice should children not feel able to protect themselves and seek redress were sufficient to balance the importance of the open court principle. If reputation is recognized as a sufficiently important value, the breach of which poses great risk and significant impact upon vulnerable individuals, perhaps Bragg would provide the necessary precedent in assisting claimants in that situation to retain their anonymity whilst seeking justice.

⁵³⁰ Daniel Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (New Haven: Yale University Press, 2007) at 121.

⁵³¹ *A.B. v Bragg Communications Inc.* [2012] SCC 46 at para 27.

CONCLUSION 5: It should be possible for people to seek to redress reputational injuries without further injuring themselves in so doing

Is Takedown Sufficient?

Daniel Solove has suggested a system akin to the *US Digital Millennium Copyright Act's* takedown provisions, that is, a law that “encourage(s) websites to develop a process by which problems can be adjudicated and resolved, where bad information can quickly be taken down and false statements can be corrected.”⁵³² Having looked at reputation in all its nuances, I do not believe that such a system could truly be effective, especially with regard to formal reputation systems. For instance, taking into account the effects of a reputation cascade⁵³³, how can “false” statements be distinguished from those that are misinformed? And when each successive review of assessment is influenced by those before it, does the removal of a single one really address the underlying issue? Can the removal of any information truly be said to be effective, in fact, in a world of data caches and widespread information dissemination? Indeed, can such subjective information as a review of assessment truly be “false”? And while defamation, both in the criminal and civil contexts, extends to inferences as well as actual text, how can corrections or takedowns be shown as demonstrably necessary if the issue is inference rather than statement? Assuming, for the moment, that such a system is determined to be appropriate, this solution still relies on a kind of responsabilization and self-policing that is troubling. Individuals would need to be constantly aware of all information about themselves and its location in order to request such a takedown. Finally, as critiques of the DMCA itself have demonstrated⁵³⁴, another problem with the takedown

⁵³² Daniel Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (New Haven: Yale University Press, 2007) at 121

⁵³³ A cascade occurs when people observe the actions of others and then make the same choice that the others have made, independently of their own private information signals. David Easley, *Networks, Crowds and Markets: Reasoning about a Highly Connected World* (Cambridge University Press 2010) 483 at 506.

⁵³⁴ See for example Derek E. Bambauer (2012) “Orwell’s Armchair” in 3:79 *University of Chicago L. Rev.* 863-944, online: <http://lawreview.uchicago.edu/sites/lawreview.uchicago.edu/files/uploads/79_3/01%20Bambauer%20ART.pdf> or Electronic Frontier Foundation, “No Downtime for Free Speech” at <<https://www EFF.org/issues/ip-and-free-speech>>.

approach is that it becomes a form of censorship. That is, ISPs, concerned with liability, begin to takedown any or all potentially problematic information without inquiring into whether it actually meets the standards of the law. While this dissertation has been concerned with critiquing and nuancing reputation, it still recognizes reputation as an important feature of social and community culture generally rather than merely an effective insurance policy for e-commerce; an approach such as this one that effectively removes or silences reputation runs counter to these positive effects. Given all these issues, it seems clear that a takedown approach is not the appropriate or most effective strategy for dealing with reputation harms.

CONCLUSION 6: It must be able to address reputational assessments, both on an individual level and at an aggregate level

Equity-based Approach

Data protection is another approach that has been suggested as possibly applicable. While data protection principles have been implicitly reviewed in the above section on Canadian privacy laws, those laws do not constitute a “pure” data protection approach. Nevertheless, the same problems arise. Cohen has critiqued data mining practices, writing that:

Data processing practices are predicated on a belief that individuals are reducible to the sum of their transactions, genetic markers, and other measureable attributes, and that these attributes are good predictors of risk and reward in future dealings. Plainly, this belief is not entirely wrong; there is much about individual behaviour that is predictable on this basis. Yet there also is much about individual behaviour that is not. Some relevant information is inherently incapable of measurement or prediction. Human motivation is internal, partly emotional, and often adventitious. The question is whether systematically ignoring this dimension of human behaviour and human potential produces policy consequences that we would rather avoid.⁵³⁵

⁵³⁵ Julie E. Cohen, "Examined Lives: Informational Privacy and the Subject as Object" (1999-2000) 52 Stanford Law Review at 1405

This same complexity – not just of behaviour but of reputation – is one of the reasons that data protection is not an effective model for addressing all the effects and implications of reputation.

In 1996, at the closing of the 18th International Data Commissioner's Conference, Ursula Franklin gave a speech that makes cogent distinctions between data protection and privacy; not just in approach, but in effect. The distinction is eloquently set out in the following passage:

I think when you discuss privacy and data protection, as you have done; there are two poles that emerge fairly quickly: does one primarily protect people, or does one protect data? Out of that polarity arise two essential climates or models which I have perceived from the discussion of your task.

There is the climate and the model of human rights that Peter Hustinx so beautifully described. All the notions of privacy can trace back their origin and validity primarily to considerations of human rights. When human rights informs the language in which the discussion amongst you, the general public, and Parliament takes place, then you speak, rightfully, about citizens and all that comes with that.

On the other hand, if the emphasis is primarily on the protection of data, one looks at a market model, one looks at an economic model, and all the things you have heard about the new economy. Then, it is the language of the market that informs your discourse. You and everybody who speaks with you, speak about consumers, about providers, about service.

While those who primarily locate themselves in the human rights climate speak about citizens, about the relationship between groups and power, those who use the market language speak primarily about stakeholders. And when one speaks about rights and obligations, the other speaks about binding contracts. When, out of the human rights climate, one derives instruments which require independent supervision, those in the market climate speak about functional analysis and choices. When one speaks about regulation and about the roots, and the moral and legal justification of law and regulation, the people using the economic model, the market language, talk about monitoring and voluntary guides.

When the human rights approach looks at infrastructures appropriate for enforcement, the people with the market mentality and language think about correcting market failures. When health and welfare data, for example, get into the wrong hands, our friends speak about correcting market failures, when I would speak about infringements of human rights. There are differences. Indeed, these are the conflicting forces that are shaping the stormy and turbulent weather that is ahead of you.⁵³⁶

The distinction Franklin makes, as well as the effects that flow from the different approaches, are crucial not just to showing how data protection approaches are insufficient to address reputation, but also in beginning to set forth a legal approach that might better address all the issues and complexities of reputation.

Thus, having shown the way that existing social prejudices and assumptions may be embedded into reputation assessments and how inferences drawn from reputation may result in discriminatory actions, it is clear that equity values must be built in to any effective regulation of reputation.

CONCLUSION 7: Reputation should not be presumed to be always available or appropriate; boundaries should be established as to when reputation assessments may be consulted and how they are used.

CONCLUSION 8: It is not enough to regulate the assessments that form the basis of reputation; the effects of reputation must also be regulated

CONCLUSION 9: An equity-based approach is imperative in order to address the potential rights issues and discrimination potential inherent in subjectivity of reputation.

Elements of the Framework

These understandings and recognitions, both about reputation itself and about appropriate systemic treatments of such question, must form the foundation of any framework that is developed. Cohen talks about needing a process that “force[s]

⁵³⁶ <http://www.priv.gc.ca/speech/archive/02_05_a_960918_05_e.cfm>.

attention over and over again to the ways that culture moves, to the ways that subjectivity is made and remade, and to the ways that the play of everyday material practice leads to technical and social innovation.”⁵³⁷ My project, in the previous chapters, has been to explore the intersections of culture, subjectivity and the play of everyday material practice with reputation. It is my hope that this can provide the necessary information for a meaningful and effective approach to the regulation of reputation to be grounded.

Any framework for reputation governance, then, must include at a minimum these factors:

1. Constitute a formal legal mode of regulation
2. The intent of the law should be aspirational, with a transformative aim rather than mere individual redress as its goal.
3. The focus of the law should relate to the derivation and use of reputation by organizations rather than placing responsibility for protection and management on the individual.
4. The scope of the law should be reputation generally, both online and offline rather than focussing only on technology or technologically-mediated or applied reputation.
5. People should be able to seek redress without being required to expose or further damage themselves in the process.
6. It is not sufficient to focus only on individual reputational assessments; since reputation is cumulative and may be technologically aggregated, the law must be able to address these forms of reputation as well.

⁵³⁷ Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press, 2012) at 268.

7. Reputation should not be presumed to be always available or appropriate; boundaries should be established as to when reputation assessments may be consulted and how they are used.
8. It is not enough to regulate the assessments or that form the basis of reputation; the effects of reputation must also be regulated.
9. An equity-based approach is imperative in order to address the potential rights issues and discrimination potential inherent in subjectivity of reputation.

Obviously, there is still work to be done in building legislation on this framework and implementing it. It is my hope that this under-labourer has performed her task; that much of the rubbish has been cleared away, the true complexity of the issue exposed, and a path has been cleared for progress, with progress markers established along that path.

Bibliography

Laws

Access to Information Act, R.S.C. 1985, c. A-1. Online <http://laws-lois.justice.gc.ca/eng/acts/A-1/>

Bill C-12 *An Act to Amend the Personal Information Protection and Electronic Documents Act* 41st Parliament, 1st Session. Online: <http://openparliament.ca/bills/41-1/C-12/>

Criminal Code of Canada R.S.C. 1985, c. C-46. Online: <http://laws-lois.justice.gc.ca/eng/acts/C-46/>

European Union, *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, 24 October 1995, available at: <http://www.unhcr.org/refworld/docid/3ddcc1c74.html>

Illinois General Assembly 2011-2012, 97th General Assembly. Bill Hb3782: Right to Privacy – Social Net.

Mental Health Parity Law (1999) SB 86 online: http://www.njleg.state.nj.us/9899/Bills/PL99/106_.PDF

OECD. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Information*. Online: http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html

Personal Information Protection and Electronic Documents Act S.C. 2000, c. 5. Online: <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html>

Privacy Act R.S.C. 1985, c. P-21. Online: <http://laws-lois.justice.gc.ca/eng/acts/P-21/index.html>

UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, online:

<http://www.unhcr.org/refworld/docid/3ae6b3aa0.html> [accessed 15 December 2012]

UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III), online:
<http://www.unhcr.org/refworld/docid/3ae6b3712c.html> [accessed 15 December 2012]

Jurisprudence

Allan v. Bushnell T.V. Co., [1969] 2 .R. 6 (C.A.)

Beye v. Horizon, 06-Civ.-5337

A.B. v. Bragg Communications Inc. [2012] SCC 46

Burton v. Crowell Publishing Co., 82 F.2d 154 (2d Cir. 1936).

Carter v Connors (2009) NBQB 317

Cassidy v. Daily Mirror Newspapers, [1929] 2 K.B. 331 (C.A.)

Cherneskey v. Armadale Publishers Ltd [1979] 1 S.C.R. 1067

Crookes v. Wikimedia Foundation Inc., 2008 BCSC 1424

Edwards v. Canada (Attorney General) [1930] A.C. 124

Foley v. Horizon, 06-Civ.-6219

Food Lion v. Melton, (1995) 250 Va. 144

Frangione v. Vandongen et al (2010) ONSC 2823

Fric v. Gersmann (2012) BCSC 614

Hall (Litigation Guardian of) v Powers [2002] O.J. No. 1803 (ON Sup. Ct. J)

Hanley v. Pisces Productions Inc., [1981] 1 W.W.R. 369 (B.C.S.C.)

Hill v. Church of Scientology of Toronto [1995], 2 S.C.R. 1130

E. Hulton & Co. v. Jones, [1910] A.C. 20 (H.L.)

Landry c. Provigo Québec Inc (Maxi & Cie), 2011 QCCLP 1802 (CanLII)

Leduc v. Roman (2009) CanLii 6838 (ON Sup. Ct)

McRae v. South Australian Telecasters Ltd. (1976), 14 S.A.S.R. 162 (S.C.)

Murphy v. Perger, [2007] O.J. No. 5511 (Sup. Ct)

Plato Films Ltd. v. Speidel, [1961] A.C. 1090 at 1138 (H.L.)

Reference re Section 94(2) of the Motor Vehicle Act, [1985] 2 S.C.R. 486

Schuster v. Royal & Sun Alliance Insurance Company (2009) 58971 (ON Sup Ct.)

Shonn's Makeover & Spa v. M.N.R. [2010] TCC 542

T.V. v. Union Township Board of Education, UNN-L-4479-04

Trinity Western University v. College of Teachers, [2001] 1 S.C.R. 772, 2001 SCC 31

Vriend v. Alberta, [1998] 1 S.C.R. 493

WIC Radio Ltd. v. Simpson [2008] 2 S.C.R. 420

Wice v Dominion Insurance of Canada (2009) 36310 (ON Sup. Ct)

Reports

Brim, Robert J. and Rhonda L. Lenton. "Love Online: A Report on Digital Dating in Canada." 6 February 2001.

<<http://www.bestsoftworks.com/docs/loveonline.pdf>>.

Electronic Privacy Information Center "Social Network Sites and Virtual Communities" in *Privacy and Human Rights Report 2006* (Washington DC, EPIC, 2007) at <<http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Social.html>>

Dr. Richard Frank et al., "Social Media Sites: New Fora for Criminal, Communication and Investigation Opportunities Public Safety Canada online at:
<<http://www.sfu.ca/iccrc/content/PS-SP-socialmedia.pdf>>

LaForest, et al. "Promoting Equality: A New Vision: Report of the Canadian Human Rights Act Review Panel." 2000.

Leger Marketing Report. "Canadians and Online Dating." 2004.
<<http://www.legermarketing.com/documents/SPCLM/040809ENG.pdf>>.

Livingstone, Sonia, and Magdalena Bober. "Uk Children Go Online: Listening to Young People's Experiences." Report 1. ESRC Project. London, 2003.
<<http://www.lse.ac.uk/collections/children-go-online/UKChildrenGoOnlineReport1.pdf>>.

Microsoft. "Online Reputation Management Survey" Data Privacy Day 2012.
<<http://go.microsoft.com/?linkid=9797152>>.

Steeves, Valerie. "Young Canadians in a Wired World, Phase II - Trends and Recommendations." Ottawa: Media Awareness Network, 2004.
<<http://www.media-awareness.ca/english/research/YCWW/phaseII/>>.

Speeches

Bernier, Chantal "Personal Data Protection Issues in a Globalized World" remarks delivered at 3d Conference of Francophonie Data Protection and Privacy Commissioners, 3 November 2009. Online:
<http://www.priv.gc.ca/speech/2009/sp-d_20091103_cb_e.cfm>.

Bernier, Chantal "Protecting Personal Information in a Globalized Environment" Speech delivered at the 2009 Access and Privacy Conference, June 12, 2009. Online: <http://www.priv.gc.ca/speech/2009/sp-d_20090612_cb_e.cfm>.

Campbell, Lisa and Daniel Caron "The Unique Challenges to Privacy Rights Caused by the Internet and Other Emergent Technologies" Internet Law Conference: The Second Wave: New Developments, Challenges and Strategies, 27-28 March 2008 online: <http://www.priv.gc.ca/speech/2008/sp-d_080327_lc_e.cfm>.

Stoddart, Jennifer "Social Networking and the New Rules of the Road" speech delivered at the IAPP Privacy Summit (30 April 2009), online:
<http://www.priv.gc.ca/speech/2009/sp-d_090430_e.cfm>.

Stoddart, Jennifer "Privacy and the Social Networking Revolution" speech delivered to the Employees of the Bank of Canada (9 September 2008) online:
<http://www.priv.gc.ca/speech/2008/sp-d_080909_e.cfm>.

Guidance Documents

Office of the Information and Privacy Commissioner of Ontario. "Reference Check: Is Your Boss Watching? Privacy and Your Facebook Profile." Information and Privacy Commissioner of Ontario.

Office of the Information and Privacy Commissioner of Ontario. "When Online Gets Out of Line" Guidance Document: Information and Privacy Commissioner of Ontario online: http://www.ipc.on.ca/images/Resources/up-facebook_ipc.pdf

Office of the Privacy Commissioner of Canada *Fact Sheet: Privacy and Social Networking in the Workplace* (May 2009) online: <http://www.priv.gc.ca/fs-fi/02_05_d_41_sn_e.cfm>

Office of the Privacy Commissioner of Canada: *Guidance Document: Electronic Disclosure of Personal Information in the Decisions of Administrative Tribunals*. Online: <http://www.priv.gc.ca/information/pub/gd_trib_201002_e.cfm>

US Department of Homeland Security *Analysts Desktop Binder*. Media Monitoring Capability Desktop Reference Binder. (2011)
<<http://www.scribd.com/doc/82701103/Analyst-Desktop-Binder-REDACTED>>

Secondary Sources: Books

Baym Nancy. *Personal Connections in the Digital Age* (Digital Media and Society, 2010).

Bentham, Jeremy. *The Panopticon Writings*, edited by Miran Bozovic (London: Verso, 1995).

- W.E Bijker, T.P. Hughes and T. Pinch. *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (Cambridge, MA: The MIT Press, 1987).
- Bogard, William. *The Simulation of Surveillance: Hypercontrol in Telematic Societies* (Cambridge, MA: Cambridge University Press, 1996).
- Brown, Raymond E. *Defamation Law: A Primer* (Toronto: Carswell, 2003).
 ———. *The Law of Defamation in Canada*, Vol. 1, *The Law of Defamation in Canada* (1987).
- Cohen, Julie E. *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press, 2012).
- Cruikshank, Barbara. *The Will to Empower: Democratic Citizens and Other Subjects* (Ithaca
 London: Cornell University Press, 1999).
- Dean, M. *Governmentality: Power and Rule in Modern Society* (London: Sage, 1999).
- Deleuze, Gilles. *Negotiations, 1972-1990*, Translated by Martin Joughin (1990).
- Doe, Jane. *The Story of Jane Doe: a book about rape* (Canada: Random House, 2003).
- Dunbar, Robin. *The Trouble With Science*. (Boston: Harvard University Press, 1996).
- Elmer, Greg. *Profiling Machines: Mapping the Personal Information Economy* (Cambridge, MA: MIT Press, 2004).
- Folkard, Henry Coleman. *The Law of Slander and Libel*, 5 ed. (London, 1898).
- Foucault, Michel. *Discipline and Punish: The Birth of the Prison* (New York: Vintage Books, 1995).
- . "Governmentality." In *The Foucault Effect: Studies in Governmentality*, edited by Graham Burchell, Colin Gordon and Peter Miller, 87-104 (Chicago: University of Chicago Press, 1991).
- Friedman, Lawrence M. *Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety and Privacy* (Stanford: Stanford University Press, 2007).

- Garfinkel, Harold. *Studies in Ethnomethodology* (New Jersey: Prentice-Hall, 1967).
- Garland, David. *The Culture of Control: Crime and Social Order in Contemporary Society* (Chicago: University of Chicago Press, 2001).
- Giddens, Anthony. *Modernity and Self-Identity* (Stanford: Stanford University Press, 1991).
- Goffman, Erving. *Interaction Ritual* (New York: Anchor Books, 1967).
- . *Presentation of Self in Everyday Life* (New York: Anchor Books, 1959).
- . *Relations in Public* (New York: Basic Books, 1971).
- Hart, H.L.A. *The Concept of Law* (Clarendon Press, 1961).
- Herman, Edward S, and Noam Chomsky. *Manufacturing Consent: The Political Economy of the Mass Media* (New York: Pantheon, 1983).
- Hess, D.J. *Science & Technology in a Multicultural World: The Cultural Politics of Facts & Artifacts* (New York: Columbia University Press, 1994).
- Hunt, H, and G Wickham. *Foucault and Law* (London: Pluto Press, 1994).
- Latour, B. *Science in Action* (Cambridge, MA: Harvard University Press, 1987).
- Lessig, L. *Code version 2.0* (New York, Perseus Books, 2006)
- Lewin, K. (1943) Psychological Ecology in *Field Theory In Social Sciences I* (New York: Harpers 1951)
- Lyon, David. *The Electronic Eye* (University of Minnesota Press, 1994).
- . *Surveillance Society* (McGraw-Hill, 2001).
- Mead, George Herbert "The Realization of the Self in the Social Situation", Section 26 in *Mind Self and Society from the Standpoint of a Social Behaviorist* (Edited by Charles W. Morris).(Chicago: University of Chicago 1934).

- Nakamura, Lisa. *Digitizing Race: visual cultures of the Internet (Electronic Mediations, University of Minnesota Press 2007).*
- Neumann, P.G. *Computer-Related Risks* (New York: ACM Press, 1995).
- Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Palo Alto, Stanford University Press, 2009).
- Nock, Steven L. *The Costs of Privacy: Surveillance and Reputation in America* (New York: Aldine de Gruyter, 1993).
- Perrin, Stephanie, and et al. *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto: Irwin, 2001).
- Razack, Sherene. *Looking White People in the Eye: Gender, Race and Culture in Courtrooms and Classrooms* (Toronto: U of Toronto Press 1998).
- Rheingold, H. *The Virtual Community* (Reading, MA: Addison-Wesley Publishing Co., 1993).
- Rose, Nikolas. *Powers of Freedom: Reframing Political Thought* (Cambridge: Cambridge University Press, 1999).
- Sacks, H. *Lectures on Conversation* (Oxford: Blackwell, 1995).
- Solove, Daniel J. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (New Haven: Yale University Press, 2007).
- Sudnow, D. *Studies in Social Interaction* (Glencoe, IL: Free Press, 1972).
- Turkle, S. *Life on the Screen: Identity in the Age of the Internet* (New York: Simon & Schuster, 1995).
- Wenger, Etienne, and Jean Lave. *Situated Learning: Legitimate Peripheral Participation* (Cambridge, MA: Cambridge University Press, 1991).
- White, Michele. *The Body and the Screen: Theories of Internet Spectatorship* (Cambridge: MIT Press, 2006).
- Yoshino, Kenji *Covering: the hidden assault on our civil rights* (Random House 2006)

Secondary Sources: Articles

Acquisti, Alessandro, and Ralph Gross. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook." Paper presented at the 6th Workshop on Privacy Enhancing Technologies, Cambridge, UK: Robinson College (June 28-30, 2006).

Albrecht, Anders. "Online Social Networking as Participatory Surveillance." *First Monday*.

Andrejevic, Mark. "The Work of Watching Each Other." *Surveillance & Society* 2, 4, 479-97.

Bailey, C. "Virtual Skin: Articulating Race in Cyberspace." *Immersed in Technology: Art and Virtual Environments*, edited by M. A. Moser (1996).

barrigar, jennifer. "Is You Is or Is You Aint: Making PIPEDA's Rights Language Meaningful by Re-Viewing Social Value." (2006).

Barton, Ben F, and Marthalee S Barton. "Modes of Power in Technical and Professional Visuals." *Journal of Business and Technical Communication* 7:1 (1993) 138-62.

Bartow, Ann. "Internet Defamation as Profit Center: The Monetization of Online Harassment" *Harvard Journal of Law and Gender* 101, 32:2 (2009).

Bailey, C. "Virtual Skin: Articulating Race in Cyberspace", M.A. Moser, ed. *Immersed in Technology: Art and Virtual Environments* 29 (1996).

Beer, David. "Social network(Ing) sites...revisiting the story so Far: A Response to danah boyd and Nicole Ellison, 13:2 (January 2008) 516.

Berzins, Christopher. "Protecting Personal Information in Canada's Private Sector: The Price of Consensus Building" *Queen's LJ* (2002).

Bhattacharya, Rajeev, Timothy M. Devinney, and Madan M. Pillutla. "A Formal Model of Trust Based on Outcomes." *The Academy of Management Review* 23: 3 (1998).

- Bloomfield, B., and T. Verdubakis. "Boundary Disputes: Negotiating between the Technical and the Social in the Development of IT Systems." *Information Technology & People* 7:1(1994).
- Bogard, William. "Surveillant Assemblages and Lines of Flight." *Theorizing Surveillance: The Panopticon and Beyond*, edited by David Lyons, 97 (2006).
- Borsook, P. "The Memoirs of a Token: An Aging Berkeley Feminist Examines Wired" *Wired Women: Gender and New Realities in Cyberspace*, edited by L. Cherney and E.R. Weise (1996).
- Bowland, Adelyn. "Sexual Assault Trials and the Protection of Bad Girls" in Julian V Roberts & Renate M Mohr eds., *Confronting Sexual Assault: A Decade of Legal and Social Change* (Toronto: University of Toronto Press, 1994).
- boyd, danah. "Social Network Sites: Public, Private, or What?" *Knowledge Tree* 13:28 (2007).
- . "Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life." In *Youth, Identity and Digital Media*, edited by David Buckingham, MacArthur Foundation Series on Digital Learning (2007).
- boyd, danah, and Jeffrey Heer. "Profiles as Conversation: Networked Identity Performance on Friendster." Paper presented at the Proceedings of the Hawai'i International Conference on System Sciences (HICSS-39), Persistent Conversation Track (2006).
- boyd, danah, and Alice Marwick. "Social Privacy in Networked Publics: Teens' Attitudes, Practices and Strategies." *Privacy Scholars Conference* (June 2011).
- boyd, danah m., and N. B. Ellison. "Social Network Sites: Definition, History, and Scholarship." *Journal of Computer-Mediated Communication* 13:1 (2007).
- Boyd, Susan. "Introduction" *The Public/Private Divide: Feminism, Law, and Public Policy*, Susan Boyd, ed. (1997).
- Brake, David. "Shaping The "Me" In Myspace: The Framing of Profiles on a Social Network Site." *Digital Storytelling, Mediatized Stories: Self-Representations in New Media*, edited by K. Lundy (2008).

- Brown, P., and S. Levinson. "Universals in Language: Politeness Phenomena." *Questions and Politeness: Strategies in Social Interaction*, edited by E.N. Goody, (1979).
- Carey, Robert F. "Mobile Telephony in Quiet Places: Territoriality and the Regulation of Noise" (2006) (unpublished).
- Castel, Robert. "From Dangerousness to Risk" *The Foucault Effect: Studies in Government Rationality*, edited by Colin Graham, Graham Burchell and Peter Miller, 281 (1991).
- Christofides, Emily, Amy Muise, and Serge Desmarais. "Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes?" *CyberPsychology & Behavior* 12: 3 (2009) 341.
- Chon, Margaret "Erasing Race? A Critical Race Feminist View of Internet Identity-Shifting" (1999-2000) *J. Gender, Race & Justice* 439-473.
- Citron, Danielle Keats. "Law's Expressive Value in Combating Cyber-Gender Harassment" *Michigan Law Review* 108:3 (2009).
- Clarke, Roger. "Beyond Oecd Guidelines: Privacy Protection for the 21st Century", online: <www.rogerclarke.com>.
- Clarke, R. "Dataveillance by Governments" *Information Technology & People* 7: 2 (1994).
- . "Human Identification in Information Systems: Management Challenges and Public Policy Issues." *Information Technology & People* 7:4 (1994).
- Cohen, Julie E. "Examined Lives: Informational Privacy and the Subject as Object." *Stanford Law Review* 52 (1999-2000).
- . "Privacy, Ideology and Technology: A Response to Jeffrey Rosen." *Geo.L.J.* 89 (2000-2001).
- Conte, Rosaria, and Mario Paolucci. "Reputation in Artificial Societies: Social Beliefs for Social Order." In *Multiagent Systems, Artificial Societies, and Simulated Organizations*, edited by Gerhard Weiss (2002).

- Correll, S. "The Ethnography of an Electronic Bar: The Lesbian Cafe." *The Journal of Contemporary Ethnography* 24 (1995).
- Corrigan, Don. "Does Kirkwood High School Have Jurisdiction over Off-Campus Internet Activity?" *St. Louis Journalism Review* (June 2006) 20-21.
- Debatin, Bernhard, et al. "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences." *Journal of Computer-Mediated Communication* 15 (2009).
- Dellaracos, C. "The Digitization of Word of Mouth: Promises and Challenges of Online Feedback Mechanisms" *Journal of Management Science* 49:10 (2003) 1407-1424.
- Dickerson, Darby. "Risk Management and the Millennial Generation." *Campus Activities Programming* (2007) A12-A16.
- DiMicco, Joan Morris, and David R. Millen. "Identity Management: Multiple Presentations of Self in Facebook" (2007).
- Dingledine, Roger, Michael J Freedom, David Molnar, David Parkes, and Paul Syverson. "Reputation" (2003).
- Donath, Judith. "Signal in Social Supernets" *Journal of Computer-Mediated Communication* 13: (2007).
- . "Identity and Deception in the Virtual Community" *Communities in Cyberspace*, P. Kellock & M. Smith, eds. (London: Routledge, 1999).
- Donath, Judith, and danah boyd. "Public Displays of Connection" *BT Technology Journal* 22:4 (2004).
- Dunn., R.G. 1997. "Self, Identity and Difference: Mead and the Poststructuralists." *Sociological Quarterly* 38.4: 687-705.
- Easterbrook, Frank L. "Cyberspace and the Law of the Horse" *U. Chicago Legal F* 207 (1996)
- Ellison, Nicole, Rebecca Heino, and Jennifer Gibbs. "Managing Impressions Online: Self-Presentation Processes in the Online Dating Environment" *Journal of Computer-Mediated Communication* 11:2 (2006).

- Escobar, A. "Welcome to Cyberia: Notes on the Anthropology of Cyberculture" *Cyberfutures: Culture and Politics on the Information Superhighway*, edited by Z. Sarder and J.R. Ravetz (1996).
- Ewald, Francois. "Insurance and Risk" *The Foucault Effect: Studies in Government Rationality*, edited by Colin Graham, Graham Burchell and Peter Miller (1991) 197.
- Fiore, Andrew, and Judith Donath. "Online Personals: An Overview" *CHI 21004*, (April 2004) 24-29.
- Flaherty, David. "Privacy in Colonial New England" *University of Virginia Press* (1972).
- Frye, Marilyn. "A Note on Anger" *The Politics of Reality* (Trumansburg, NY: Crossing Press, 1983)
- Fusco, Caroline. "Inscribing Healthification: Governance, Risk, Surveillance and the Subjects and Spaces of Fitness and Health." *Health and Place* 12 (2006).
- Gajjala, Radhika and Annapurna Mamidipudi, "Gendering Processes Within Technological Environments: A Cyberfeminist Issue" (Spring 2002 Rhizomes (4), online: <<http://www.rhizomes.net/issue4/gajala.htm>>.
- Gallagher, Mary Pat. "Myspace, Facebook Pages Called Key to Eating Disorder Coverage Dispute" *New Jersey Law Journal* (2008). online at: <<http://www.law.com/jsp/pa/PubArticlePA.jsp?id=900005502531>>.
- Gavison, Ruth "Feminism and the Public/Private Distinction", 45 *Stan. L.R.* 1 (1992).
- Giddens, Anthony. "Risk and Responsibility" *The Modern Law Review* 62:1 (1999).
- Gottlieb, Henry. "Myspace, Facebook Privacy Limits Tested in Emotional Distress Suit" *New Jersey Law Journal*, (June 7, 2007).
- Grimmelmann, James. "The Unmasking Option" *Denver University Law Review Online*. (Jan. 2010) 23, online: <http://works.bepress.com/james_grimmelmann/29>.

- Haggerty, Kevin D. and Ericson, Richard V. "The Surveillant Assemblage" *British Journal of Sociology* 51:4 (2000) 605-22.
- Hammack, Phillip L. "Narrative and the Cultural Psychology of Identity" *Personality and Social Psychology Review* 12 (2008).
- Henman, Paul. "Targeted! Population Segmentation, Electronic Surveillance and Governing the Unemployed in Australia." *international Sociology* 19:2 (2004) 173-91.
- Joinson, Adam N. "Looking at, Looking up, or Keeping up with People? Mothers and Use of Facebook." *SIGGHI* (2008) 1027-1036.
- Jones, Jenny. "Reproduction and the Creation of the Digital Image" *N. Paradoxa: international feminist art journal* 9 (1999).
- Kendall, Lori. *Hanging Out in The Virtual Pub: Masculinities and Relationships Online* (Berkeley: University of CA Press, 2002).
- Kerr, D. "Beheading the King and Enthroning the Market: A Critique of Foucauldian Governmentality" *Science & Society* 63:2 (1999) 173-203.
- Kerr, Ian. "The Strange Return of Gyges' Ring: An Introduction." *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford, Oxford University Press, 2009).
- Kerr, Ian, Jennifer Barrigar, Jacquelyn Burkell, and Katie Black. "Soft Surveillance, Hard Consent" *Lessons from the Identity Trail* (London: Oxford University Press, 2009).
- Klein, Daniel, and Jeremy Shearmur. "Good Conduct in the Great Society: Adam Smith and the Role of Reputation" *Reputation: Studies in the Voluntary Elicitation of Good Conduct*, edited by Daniel B. Klein, 29 (1997).
- Klein, Daniel B. "Promise Keeping in the Great Society: A Model of Credit Information Sharing" *Reputation: Studies in the Voluntary Elicitation of Good Conduct*, edited by Daniel B. Klein (1997).

- . "Trust for Hire: Voluntary Remedies for Quality and Safety" *Reputation: Studies in the Voluntary Elicitation of Good Conduct*, edited by Daniel B. Klein, 97 (1997).
- Kramer, Nicole C, and Stephan Winter. "Impression Management 2.0: The Relationship of Self-Esteem, Self-Efficacy and Self-Presentation within Social Networking Sites" *Journal of Media Psychology* 20:3 (2008).
- Lampe, Cliff, Nicole Ellison, and Charles Steinfield. "A Familiar Face(Book): Profile Elements as Signals in an Online Social Network" (2007).
- Larsen, Marlene Charlotte, "Understanding Social Networking: On Young People's Construction and Co-Construction of Identity Online" *Association of Internet Researchers: Let's Play* (2007).
- Lemke, Thomas. "The Birth of Bio-Politics: Michael Foucault's Lectures at the College De France on Neo-Liberal Governmentality" *Economy and Society* 30:2 (2001) 190-207.
- . "Foucault, Governmentality, and Critique" *Rethinking Marxism* 14:3 (2002) 49-64.
- Lerman, Kristina. "Social Networks and Social Information Filtering on Digg" (2006).
- Lianos, Michalis. "Social Control after Foucault" *Surveillance & Society* 1:3, 412-30.
- Liu, Hugo. "Social Network Profiles as Taste Performances" *Journal of Computer-Mediated Communication* 13:1 (2007).
- Locke, John. "An Epistle to the Reader" *An Essay Concerning Human Understanding*, 9, ed. P. Nidditch, (Oxford, Clarendon Press, 1975).
- Los, Maria. "Looking into the Future: Surveillance, Globalization and the Totalitarian Potential" *Theorizing Surveillance: The Panopticon and Beyond*, 69, edited by David Lyons (2006).
- Lyon, David. "9/11, Synopticon, and Scopophilia: Watching and Being Watched" *The New Politics of Surveillance and Visibility*, edited by Kevin Haggerty and Richard Ericson, (Toronto: University of Toronto Press, 2006) 35-54.

- . "Liquid Surveillance: The Contribution of Zygmunt Bauman to Surveillance Studies" *International Political Sociology* (2010) 4 325-338.
- Marwick, Alice. "The Public Domain: Social Surveillance in Everyday Life" *Cyber-Surveillance in Everyday Life: An International Workshop* (2011).
- . "Selling Your Self: Online Identity in the Age of a Commodified Internet" *University of Washington* (2005).
- Marx, Gary. "Ethics for the New Surveillance." *Information Society* 14:3 (1998) 171-186.
- . "Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information - 'Hey Buddy Can You Spare a DNA'" *Surveillance and Security: Technological Politics and Power in Everyday Life*, edited by T Monahan (London: Routledge, 2006).
- Massum, Hassan and Yi-Cheng Zhang. "Manifesto for the Reputation Society" *First Monday* (2004) 9.
- Mathieson, Thomas. "The Viewer Society" *Theoretical Criminology* 1:2 (1997).
- Mayer, Roger, James H Davis, and David F Schoorman. "An Integration Model of Organizational Trust" *The Academy of Management Review* 20:3 (1995).
- McLaughlin, M.L., K.K. Osborne, and N.B. Ellison. "Standard of Conduct on Usenet" In *Cybersociety: Computer-Mediated Communication and Community*, edited by S.G. Jones (1995) 90.
- Merry, Sally Engle. "Rethinking Gossip and Scandal" *Reputation: Studies in the Voluntary Ellicitation of Good Conduct*, edited by Daniel B. Klein (1997) 47.
- Mitchell, Lawrence E. "Understanding Norms" *University of Toronto Law Journal* 49 (1999).
- Myers, D. "Anonymity Is Part of the Magic" *Qualitative Sociology* 10:3 (1987).
- Nissenbaum, Helen. "Securing Trust Online: Wisdom or Oxymoron?" *B.U.L.Rev.* 81 (2001).

- O'Brien, Jodi "Writing in the Body: Gender (RE)Production in Online Interaction" *Communities in Cyberspace*, O. Kellock & M.A. Smith, eds. (London: Routledge, 1999).
- Olsen, Frances "Feminist Critiques of the Public/Private Distinction", 10 *Constitutional Commentary* 319-27 (1993).
- Pateman, Carole "Feminist Critiques of the Public/Private Dichotomy" *Public and Private in Social Life* 281, S.I. Benn and G.F. Gaus eds. (1983).
- Pearson, Erika. "All the World Wide Web's a Stage: The Performance of Identity in Online Social Networks" *First Monday* 14:3 (2009).
- Peled, Elad. "Should States Have a Legal Right to Reputation? Applying the Rationales of Defamation Law to the International Arena" *Brooklyn Journal of International Law* 35:1 (2010).
- Peluchette, Joy, and Katherine Karl. "Social Networking Profiles: An Examination of Student Attitudes Regarding Use and Appropriateness of Content" *CyberPsychology & Behavior* 11:1 (2008).
- Post, Robert. "The Legal Regulation of Gossip: Backyard Chatter and the Mass Media" *Good Gossip*, edited by Robert F. and Aaron Ben-Ze'ev Goodman (1994) 65.
- Raab, Charles D, and Colin J Bennett. "Taking the Measure of Privacy: Can Data Protection Be Evaluated?" *International Review of Administrative Science* 62:4, 535 (1 December 1996).
- Richter , Wolf, Escher, Tobias and Bray, David A., The Performance of Distributed News Aggregators (November 17, 2008). OII DPSN Working Paper No. 9 , online, SSRN: <<http://ssrn.com/abstract=1324462>>.
- Rose, Nikolas. "The Death of the Social? Re-Figuring the Territory of Government" *Economy and Society* 25:3 (1996).
- . "The Politics of Life Itself" *Theory, Culture & Society* 18:6 (2001).
- Rose, Nikolas, and Peter Miller. "Political Power Beyond the State: Problematics of Government" *British Journal of Sociology* 43:2 (1992) 173-205.

- Schegloff, E. "Notes on a Conversational Practice: Formulating Place" *Studies in Social Interaction*, edited by D.N. Sudnow (1972) 75.
- . "Reflections on Talk and Social Structure" *Talk & Social Structure*, edited by D. Boden and D.H. Zimmerman (1991).
- Schwartz, Paul M. "Privacy and Democracy in Cyberspace" *Vand. L. Rev.* 52 (1999).
- Senft, T. "Dissertation Remarks and Synopsis" (2004).
- Shaw, Rhonda "Our Bodies, Our Selves, Technology and Questions of Ethics: Cyberfeminism and the Lived Body" *Australian Feminist Studies* 18:40 (2003) 45-55.
- Silver, David. "Looking Backwards, Looking Forward: Cyberculture Studies 1990-2000" *Web Studies: Rewiring Media Studies for the Digital Age*, edited by David Gauntlett, (2000) 19.
- Skrabanek, Petr. "The Death of Humane Medicine and the Rise of Coercive Healthism" *Social Affairs* (1994).
- Solove, Daniel. "The Virtues of Knowing Less: Justifying Privacy Protections against Disclosure." *Duke Law Journal* 53 (2003-4).
- Spears, R., and M. Lea. "Panacea or Panopticon? The Hidden Power in Computer-Mediated Communication" *Communication Research* 21:4 (1994).
- Stomblor, Mindy. "Buddies or Slutties: The Collective Sexual Reputation of Fraternity Little Sisters" *Gender & Society* 8:3 (1993).
- Strahilevitz, Lior Jacob. "How's My Driving? For Everyone and Everything." *New York University Law Review* 81 (2006).
- . "A Social Networks Theory of Privacy" *University of Chicago Law Review* 72 (2005).
- Stutzman, Fred. "How Facebook Broke Its Culture" *Unit Structures* (2006).
- Sunden, Jenny "What Happened to Difference in Cyberspace? The (Re)Turn of the She-Cyborg" (2001) *Feminist Media Studies*, 1:2 215-232.

- Sunstein, Cass. "Group Judgements: Statistical Means, Deliberations, and Information Markets" *New York University Law Review* 80 (2006).
- . "Infotopia: How Many Minds Produce Knowledge" *Oxford University Press* (2006).
- Sutherland, Kate. "The Impact of the Tort of Defamation on Public Discourse About Racism" *Critical Torts*, edited by Rakhi Ruparelia, Sandra Rogers and Louise Belanger-Hardy (2009) 135.
- Taylor, James, and Lewis Grimmelmann. "The Unmasking Option" *Denver University Law Review Online* (2010).
- Tsuneki, Atsushi, and Yoshinobu Zasu. "On the Complementarity between Law and Social Norm: A Model Analysis with Special Reference to the Liability Rule for Tort" *Osaka University - Institute of Social and Economic Research Discussion Paper No. 765* (2010).
- Tufekci, Zeynep. "Grooming, Gossip, Facebook and Myspace: What Can We Learn About These Sites from Those Who Won't Assimilate?" *Information, Communication & Society* 11:4 (2008).
- Vaz, Paula, and Fernanda Bruno. "Types of Self-Surveillance: from abnormality to individuals 'at risk'" *Surveillance & Society* 1:3 (2003) 272-91.
- Vitak, Jessica Marie. "Facebook "Friends": How Online Identities Impact Offline Relationships" *Georgetown University* (2008).
- Weintraub, Jeff. "The Theory and Politics of the Public/Private Distinction" *Public and Private in Thought and Practice: Perspectives on a Grand Dichotomy* 1, Jeff Weintraub & Krishan Kumar, eds. (1997).
- Wilson, F. "Managerial Control Strategies within the Networked Organization." *Information Technology & People* 8:3 (1995).
- Wu, Fang, and Bernardo A. Huberman. "Novelty and Collective Attention" *PNAS* 104:45 (2007).

Wynn, E., and J.E. Katz. "Hyperbole over Cyberspace: Self-Presentation & Social Boundaries in Internet Home Pages and Discourse" *The Information Society* (1997).

Yoshino, Kenji. "Assimilationist Bias in Equal Protection: The Visibility Presumption and the Case of 'Don't Ask, Don't Tell'" *Yale Law Journal* 108 (1998-99) 485-572.

Online: Blogs, Articles & Resources

Barker, Jeremy. "Facebooking with the Enemy" *National Post* (2008)

Brodkin, Jon. "French Court Frowns on Google Autocomplete Issues \$65,000 Fine", online: <<http://arstechnica.com/tech-policy/news/2012/01/french-court-frowns-on-google-autocomplete-issues-65000-fine.ars>>.

Canadian Press, "Court sides with two Calgary university students in Facebook free-speech case " *Globe & Mail* (9 May 2012), online: <http://www.theglobeandmail.com/news/national/court-sides-with-two-calgary-university-students-in-facebook-free-speech-case/article4105844/>.

Chalfant, Drew. "Facebook Postings, Photos Incriminate Dorm Party-Goers" *The Northener* (2005-11-02).

Dictionary.com. "Surveillance", online: <<http://dictionary.reference.com/browse/surveillance>>.

Dictionary.com. "Jurisprudence", online: <<http://dictionary.reference.com/browse/jurisprudence?s=t>>.

Digg.com. "How Digg Works", online: <<http://about.digg.com/how>>.

Dillow, Clay. NYPD Creates Facebook-Police Taskforce to Mine Social Media for Clues *PopSci* (2011), online: <<http://www.popsci.com/technology/article/2011-08/nypds-facebook-police-mine-social-media-clues-about-crime>>.

Douglas, Nick. "What the Hell Are 4chan, Ed, Something Awful and B?" *Gawker.com* (2008).

Dukowitz, "Out on Myspace, Then Out the Door" (6 June 2006):964 *The Advocate* online: <<http://www.questia.com/read/1G1-147258577/out-on-myspace-then-out-the-door-think-that-no-one>>.

eBay. "Why Leave Feedback?" *How Feedback Works*.

Fake, Caterina. "Participatory Media and Why I Love It (and Must Defend It), Response to WSJ Piece" *Huffington Post* (2010), online: <http://www.huffingtonpost.com/caterina-fake/participatory-media-and-w_b_428053.html>.

Financial Week. Facebook a Risky Tool for Background Checks, Lawyers Warn. (11 March 2008), online: <<http://www.financialweek.com/apps/pbcs.dll/article?AID=/20080311/REG/234697944>>.

Gregory, John. "Can a Google Search Suggestion Be Defamatory?" <http://www.slaw.ca/2012/02/03/can-a-google-search-suggestion-be-defamatory/?utm_source=dlvr.it&utm_medium=twitter>.

Grossman, Lev. "Time's Person of the Year: You" *Time Magazine* (2006).

Haas, N. "In Your Facebook.Com." *New York Times* (8 January 2006), online: <<http://www.nytimes.com/2006/01/08/education/edlife/facebooks.html?pagewanted=all&r=0>>.

Hanson, Aric. "Don't Ask, Don't Tell, Don't Blog, Don't Enlist: How the Internet Has Affected the Military's Policy on Gays and Lesbians" *The Revealed I*, (University of Ottawa, 2007).

Hockert, Amy "Employers Use "Facebook" and "MySpace" to Weed Out Applicants," September 9, 2006 <<http://www.wtlv.com/tech/news/news-article.aspx?storyid=64453>>.

Huffington Post. "Marisol Simoes Jailed: Co-Owner of Kinki and Mambo in Ottawa Gets 90 Days for Defamation." <http://www.huffingtonpost.ca/2012/11/16/marisol-simoes-jailed_n_2146205.html>.

Hunt, Tara. "The Whuffie Factor", online: <<http://www.thewhuffiefactor.com/>>.

Independent, The. "Taxman Admits to Facebook Trawl" *The Independent* (2008).

Kari, Shannon. "Facebook Comes to a Head" *National Post* (15 March 2008), online: <<http://www.oacas.org/news/08/march/15fbbook.pdf>>.

Lexis-Nexis, News Release, Role of Social Media in Law Enforcement Significant and Growing (18 July 2012), online: <<http://www.lexisnexis.com/media/press-release.aspx?id=1342623085481181>>.

Linksandlaw.com. Links&Law: Don't Google Job Applicants in Finland. (4 May 2007), online: <<http://www.linksandlaw.com/news-update49-job-applicants-finland.htm>>.

Long, Murray *Privacy Scan* 2008.

MacManus, Richard. "Interview with Digg Founder Kevin Rose" *ZDNet* (2006).

Miller, Colin, "Facebook Status -- Exonerated: Suspect's Facebook Update Corroborates Alibi In Brooklyn Robbery" *Evidence Prof Blog* (13 November 2009), online: <<http://lawprofessors.typepad.com/evidenceprof/2009/11/i-have-written-several-posts-on-this-blog-herehereherehere-andhere-about-cases-dealing-with-the-admissibility-of-eviden.html>>.

Moore, Matthew. "Gay Men 'Can Be Identified by Their Facebook Friends'" *The Telegraph* (2009).

Pagan, Daniel. "The Line between Sharing and Cheating" (2008)

Public Service Alliance Canada, BC Chapter. "The Facebook Trap!" (2007).

Saunders, Alec. "A Privacy Manifesto for the Web 2.0 Era" *GigaOM Blog* (2008).

Scott, Taylor. "Social Media Valuable Source for Police" *London Free Press* (9 August 2012).

Seymour, Andrew "Restauranteur Gets 90 Days in Jail for Criminally Libelling Author of Review (16 Nov 2012) Ottawa Citizen, online: <http://www.ottawacitizen.com/life/Restaurateur+gets+days+jail+criminally+libelling+author+review/7560754/story.html>.

Slade, Daryl. "University Defends Right to Discipline Students Who Criticized Prof on Facebook" *Vancouver Sun* (2011).

Smith, Russell Scott. "Onan the Vegetarian: The Story of a Raw Food Guru Turned Subway Pervert" *New York Magazine* (2006).

Sobchak, V. "New Age Mutant Ninja Hackers: Reading Mondo 2000" *South Atlantic Quarterly* 92:4 (1993).

"Taxman Admits to Facebook Trawl" The Independent (25 February 2008) online:
<<http://www.independent.ie/national-news/taxman-admits-to-facebook-trawl-1297118.html>>.

"Trend Watch: Teens Leaving Facebook for Twitter: Here's Why" *Barking Robot* (29 January 2012), online:
<<http://www.debaird.net/blendededunet/2012/01/teens-leaving-facebook-for-twitter-heres-why.html>>.

Y2U. "Wiki: Facebook