SECURING CYBERSPACE: NEO-LIBERALISM, RISK AND CHILD SAFETY

By

WADE WALLACE DEISMAN, B.A., M.A.

A thesis submitted to
The Faculty of Graduate Studies and Research
in partial fulfillment of
the requirements for the degree of

Doctor of Philosophy

Department of Sociology and Anthropology

Carleton University

Ottawa, Ontario

January 2008

© copyright

2008, Wade Wallace Deisman

Library and Archives Canada

Published Heritage Branch

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque et Archives Canada

Direction du Patrimoine de l'édition

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence
ISBN: 978-0-494-40520-8
Our file Notre référence
ISBN: 978-0-494-40520-8

NOTICE:
The author has granted a non-exclusive license allowing Library and Archives Canada to reproduce, publish, archive, preserve, conserve, communicate to the public by telecommunication or on the Internet, loan, distribute and sell theses worldwide, for commercial or non-commercial purposes, in microform, paper, electronic and/or any other formats.

The author retains copyright ownership and moral rights in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

AVIS:
L'auteur a accordé une licence non exclusive permettant à la Bibliothèque et Archives Canada de reproduire, publier, archiver, sauvegarder, conserver, transmettre au public par télécommunication ou par l'Internet, prêter, distribuer et vendre des thèses partout dans le monde, à des fins commerciales ou autres, sur support microforme, papier, électronique et/ou autres formats.

L'auteur conserve la propriété du droit d'auteur et des droits moraux qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this thesis.

While these forms may be included in the document page count, their removal does not represent any loss of content from the thesis.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de cette thèse.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.

Canada

Abstract

"CARLETON UNIVERSITY"

Securing Cyberspace: Neo-liberalism, Risk and Child Safety

Abstract

Drawing upon risk and governance literatures and the social construction of technology approach (SCOT), this work explores the processes by which cyberspace was transformed in the name of securing children. Much research on the Internet's early development has focused on questions of criminal liability, leaving the impression that states were plenipotentiary steering agents. This analysis provides a corrective, de-centering the state and focusing instead on social responses to perceived threats to children and their impact. I describe the emergence of a wide-scale process of problematization in response to the presence of cyber-predators, pornographers and pedophiles in cyberspace. This process culminated in the formulation of a distinctly neo-liberal, risk inflected 'problematic' that: 1) reframed threats as risks manageable through prevention and precaution; 2) functioned as a call for action across a variety of institutional contexts; and 3) served as a call to arms to a variety of non-state actors. Two larger anxieties contributed to the dissemination of this problematic, investing it with additional potency and increasing its likelihood of uptake: a generalized worry about the welfare of children associated with neo-liberalism, and a deeper anxiety associated with the pace of technological change characteristic of risk societies. Drawing upon SCOT, the investigation traces the arc of this problematic across three action contexts, describing its process of uptake by actors and their assorted problem-solving strategies. The term securitization, which denotes logics of action which aim to reduce risk by acting on its conditions of possibility, is used to broadly characterize the processes underway in each distinct domain (design, operations, and emplacement) while tactics unique to each are explored. Design contexts involve attempts to enhance child security through built-in hardware or software protections. The second domain, denoted as operations, securitization is achieved either through direct action in cyberspace or by attempting to mediate the ways that other people act in cyberspace. In the third context, emplacement, securitization works through strategies of responsibilization. The work concludes by arguing that securitization efforts across these domains had the cumulative effect of altering both the nature of cyberspace as well as the Internet's future trajectory of technological development.

Acknowledgements

I would like to express my gratitude to many people in the Department. Most importantly I want to thank Aaron Doyle for agreeing to take me on at such a late date, and under such difficult circumstances. This work could not have come to fruition without his commitment, support, and patience. I also owe an immense debt of gratitude to Peter Swan for his unswerving confidence over all these years and for always being ready to share his thoughtful reflections. His unflagging confidence in me sustained me and provided the encouragement I needed to finish. Neil Gerlach also deserves thanks for agreeing to stand in as a third committee member on such short notice and for taking up the challenge with enthusiasm. Sean Hier is to be thanked for his diligence as an external reviewer.

During my time at Carleton I benefited greatly from the guidance and generosity of many wonderful people. Janet Siltanen and Wallace Clement set our cohort out on a sturdy and sustainable course and nurtured our spirits and souls along the way. Alan Hunt proved a valuable sparring partner and was not above trying to call me to order. Rob Shields made several opportunities available to me early on and was a reliable interlocutor. Bruce Curtis taught me to think in new ways and with the cunning of reason. Of Jacques Chevalier, I can only say that the opportunities he offered me to expand my pedigree were invaluable. Craig McKie was always a confidant and engaging thinker.

I made many friends along the way and hence, have many friends to thank. Kevin Selbee's passion, enduring friendship and brotherly love were vital. Mary Stratton has provided critical unflinching support. Valerie De Courville and Heidi Rimke were dear friends to me in the formative stages of my intellectual journey. I am also grateful to June Madeley, who stood by me till the very end.

Many people stood off to the sidelines in terms of the often gruelling day in and day out drama of finishing, but nonetheless offered their moral support and solicitude. This is true of my friends at the Law Commission of Canada: Natalie Des Rosiers, Denis Coley, Bruno Bonneville, and most especially Susan Zimmerman and Annie Di Palma. Dominique Robert, Martin Dufresne, Michael Kempa, Christine Gervais, Kathryn Campbell, and Myriam Denov, and many other friends at the University of Ottawa also deserve thanks for making themselves available as sounding boards or simply providing support.

Throughout the process of working toward the completion of this thesis I have been teaching full time at the University of Ottawa. Over this period I have had the great privilege of getting to know some truly great people. Time and time again, when my patience or interest in finishing was flagging, it was the contact with students that brought me back to centre, grounding me and reminding me that it was worthwhile. In this regard, I also owe a particularly large debt of gratitude to the many dedicated members of the National Security Working Group.

Acknowledgements

Finally, I should like to thank my family for keeping the faith throughout the duration and always standing by me. Nora and Tara, Todd and Guy, Zander and Kayden, Mark and Leni – near me always and dearer than words can say.

My last words of thanks and gratitude are for Shannon Tucker who has been an unimaginable source of joy in my life, acted as my most loyal and unflagging comrade in the final stages of the battle, and whose bright sunshine, phenomenal strength and wonderful spirit have been a saving grace. This work is dedicated to her.

Table of Contents

Table of Contents (Continued)

Chapter IV: Problem Solving and Socio-Technical Solutions

Chapter V: Design Contexts: Securitization through Embedding

Chapter VI: Contexts of Operation: Interveners and Intermediaries

Table of Contents (Continued)

Chapter VII: Modes of Securitization in Context of Emplacement

Chapter VIII: Conclusion

List of Figures

List of Tables

List of Appendices

Chapter One

The Advent of the Internet and the Social Construction of Insecurity

1.0 Introduction

Beginning roughly around the mid-eighties, pundits, futurists, technophiles, and commentators from all walks of life began to make bold and sweeping proclamations about the emergence of a new, unregulated technology, a veritable 'wild west' of free speech and pure democracy which would forever change both the way people communicated and irrevocably alter the structure of human societies and governments. The development that prompted such Promethean, even Pollyanna pronouncements, was of course, the Internet, a complex capillary computer communications network that not only operated in such a way as to ignore borders, but reached right around the world, thereby foretelling the formation of a new global village and renewing the promise of a world society based on direct democracy[1] (Kinney 1996; Kingwell 1996; Sobchack 1996; Bynum 2005).

Of course, new technologies are often ushered in by a honeymoon period. The salad days of cyberspace were no exception. As the quixotic fever faded, two provocative questions with respect to the future of the Internet remained

[1] Of course, the 'Internet' existed prior to this period, though few actually had firsthand experience with it and fewer still had regular access to the network. In the late 1980s and early 1990s, however, as infrastructure and architecture expanded and technical advances brought increased accessibility, things began to change. A general history of the development of Internet in Canada falls beyond the purview of the current investigation. In fact, there is very little in the way of current work in the Canadian context that addresses the Internet's history of development.

outstanding. Public perceptions in regard to each would have a significant impact on subsequent decisions with respect to the new medium's future. The first question focussed upon whom, if anyone, ought to have the authority to control and regulate the new medium. Even as nation states began to eye up the space and ponder questions of control, opponents of such encroachment were mobilizing to oppose such efforts. The cause of independence would be championed by an assorted collection of Internet devotees who styled themselves 'digital libertarians' (Barlow 1996).[2] They argued that the authority of the state to make and enforce law was limited to the physical territories over which it had established sovereignty and dominion, and more to the point, that cyberspace was not a physical space at all. The Internet, according to proponents of this position, was a sovereign space and ought to be allowed to develop its own internal, indigenous, organic governing mechanisms, free from the machinations of monolithic governments and bureaucratic interference (Boyle 1997:29).

A second and closely related question that had actually surfaced during the honeymoon period, but remained outstanding afterward, concerned how the rule of law and particularly criminal sanction could be applied in cyberspace at all (Biegel 2003). Prominent commentators concurred that doing so would be very difficult. Others, informed by an essentialist understanding of the nature of the new network, argued that the *sui generis* structure of the Internet made it impervious to the rule of law anyway, and thus that traditional law enforcement

---

[2] John Perry Barlow's 'A Declaration of the Independence of Cyberspace' is emblematic here.

means and mechanisms would prove ineffective (Kingwell 1996). Although doubts around this second question would be answered in time, by both a series of legislative initiatives regarding the Internet and by the successful prosecution of several criminal cases against a number of actors in cyberspace, they nonetheless had a sobering impact on early perceptions of the Internet and especially upon early portrayals of the dangers that might accompany its emergence. Indeed, while the very susceptibility of cyberspace to the rule of law remained in question, 'cybercrime' came to be seen as a particularly pernicious category of criminal conduct which might pose a serious threat to the social order in so far as, absent any effective means of address, it seemed to pose the potential for illegality with impunity.[3] One of the most mortifying embodiments of this threat appeared in the personification of cyberspace as a place where pedophiles, child predators, and child pornographers could roam freely, plying their trade without care or concern, trolling for victims and augmenting their collections at will.[4]

Fast forward ten years. Although worries about the safety of children in cyberspace have not abated, there is no longer any doubt about the capacity of

---

[3] In relation to this second issue, a body of research has since developed devoted to acknowledging the difficulties of policing cyberspace, to identifying the difficulties associated with applying the power of criminal sanction in cyberspace, and to establishing specific means and measures by which such application might be achieved (Sussman 1995; Wall 1999; Grabosky 2001). A considerable volume of research has also been addressed to the idea of virtual crime itself (Brenner 2003; Capeller 2001), to defining the forms such crime might take, and to identifying the challenges associated with addressing it (Greenleaf 2003).

[4] I have not undertaken to document all of the instances in which cyberspace was portrayed in such a way. However, I would reference an especially noteworthy example. The July 3, 1995 issue of Time Magazine featured a young child on its cover (in text). The article inside was written by Philip Elmer-DeWitt.

nation states to apply the rule of law over the Internet and to bring criminal sanction to bear in cyberspace.[5] Indeed, police in North America and Europe have charged and convicted a significant number of people for computer crimes related to children. Furthermore, police in both contexts have orchestrated far-reaching operations aimed at stemming the distribution of child pornography and at catching pedophiles and child predators operating online.[6] An extensive and complex array of cooperative law enforcement networks characterized by sundry strategies and tactics[7] have formed. Furthermore, in both contexts, the courts have held that existing laws related to child pornography and associated criminal acts apply in cyberspace[8]. In addition, a significant body of case law has developed to address a variety of related online crimes (Geist 2002). Finally, in cases where the Internet has presented new opportunities for criminal action and existing criminal procedures and provisions have been deemed wanting, new

---

[5] I do not mean to imply here that the issues are not complicated, that they are unambiguous, or that they have largely been resolved. Rather – I mean simply that courts in the United States and Canada have not taken the position that cyberspace is non-jurisdictional and that there have been a variety of prosecutions that confirm this position in both contexts.

[6] For example, In the United Kingdom there was 'Operation Ore' in 1999. The U.S. saw 'Operation Avalanche' in 2001 and 'Operation Candyman' in 2002.

[7] For example, the Guardia in Ireland began a series of investigations in the spring of 2002 (under an initiative they nominated 'Operation Amethyst') on the basis of information received from the FBI. Furthermore, 'Operation Falcon' (which was announced by the Department of Justice in the United States in January of 2004) brought together the F.B.I., the Bureau of Immigration and Customs Enforcement, the U.S. Internal Revenue Service, the U.S Air Force, the U.S Army, the U.S. Coast Guard, the U.S. Navy, and the U.S. Postal Service. The operation identified an American company that provided credit card support to a number of sites physically located in the former Soviet Union, as well as customers. The FBI's investigation in 'Operation Falcon' lead to 'Operation Auxin' in Australia which saw almost 200 people charged.

[8] European responses have been more varied. Germany passed a comprehensive legislative package which specifically addresses the Internet, while countries like France and England have adopted a more disjointed and incremental approach. The European Union has also played a leading role in such areas.

classes of crimes have been created and older definitions of criminal acts have been modified to address their online form.[9] While some of these legislative efforts have not survived constitutional challenge – as witnessed in the cases of the Communications Decency Act and the Child Online Protection Act in the United States – there is nonetheless now a significant body of law and jurisprudence devoted to establishing tests of jurisdiction and application.

If sheer numbers of convictions alone were not sufficient to dispel any lingering doubts about whether nation states have been able to wield their power and exercise authority over cyberspace, one could also marshal a plethora of other executive initiatives and regulatory measures currently in place which add force to the aforementioned juridical and legislative edifice. In contexts where telecommunications and cable companies are the primary information service providers, they have been charged with establishing their own codes of industry conduct and appropriate regimes of regulation for users. Canadian and U.S. governments have charged Internet Service Providers (ISPs) with the responsibility of developing terms of use for users and Internet Content Providers (ICPs).[10] In the Canadian context, the Coalition of Internet Service Providers (CISP) has developed the Internet Protection Portal dedicated to enhancing the safety of children in cyberspace through the use of public education materials

---

[9] In Canada, for example - Bill C-15A, an act to amend the Criminal Code with respect to the sexual exploitation of children on the Internet, received royal assent in June 2002. Also, Section 172.1 was added to criminalize electronic communication with a person believed to be a child for the purpose of facilitating the commission of sexual offences. England and Wales passed the Sexual Offences Act in 2003 to address grooming offences. Scotland passed similar laws in 2005.

[10] See Geist (2002) for a more extensive comparative discussion which encompasses various aspects of case law.

and awareness campaigns. Furthermore, governments in both countries have been engaged in supporting and fostering the development of non-state and third sector agencies mandated to develop policies, programs and other initiatives aimed at securing children in cyberspace.[11]

When all these measures and means are arrayed together, the power of law over the Internet and the efficacy of criminal sanction in cyberspace may seem so clear and so unequivocal that we may be led to wonder how anyone could ever have doubted it or imagined it could somehow have been otherwise. To do so, however, would be to fall prey to what E.P. Thompson (1963) called (in another context) the 'enormous condescension of posterity' in so far as we might then be inclined to see those who did doubt it as misguided or irrational and perhaps even to gloss over or treat this particular period (when the Internet's susceptibility to the rule of law was in question) as merely incidental, or alternatively still, to interpret it as a period of growing pains that had to be borne as part and parcel of a maturation process.

The temptation to such condescension must be avoided as a matter of principle, of course. But there is another, much more compelling reason why we ought not to rush to judgment or treat the preoccupation with child safety that characterized this early period in the Internet's historical development in a cavalier fashion. Namely, because by doing so, we risk losing sight of the fact that, in response to these preoccupations, cyberspace itself underwent a process of profound and decisive transformation. If we lose sight of this fact, we may miss

---

[11] In Canada, the most exemplary institution in this respect is probably the Media Awareness Network.

out on a key opportunity to better understand both the nature of technological change and the role and impact of the decisions we make in relation to it.

This thesis contends that the processes of securitization that the Internet underwent over this period, though not widely recognized nor well understood, nonetheless had a decisive impact on the newly emerging medium. It describes the conditions which gave rise to, and some of the key processes by which, the character of cyberspace was broadly transformed in the name of protecting the safety of children. Its aim is to understand why concerns about the welfare of children in cyberspace surfaced in the first place, how they were conceptualized and framed by relevant social actors and groups, and how, in the process of responding to and attempting to address these concerns, both the medium itself and associated social, economic, and political relations were transformed.[12]

The investigation embarked upon in this work derives from and relies for its direction on a line of questioning opened up by the social construction of technology approach. Namely, 'why did this particular problematization arise in relation to this technological system and why was this particular approach to its solution adopted and not some other approach to its solution?' (Bijker *et al.* 1987). The social construction of technology approach is particularly recommended because it aims to arrive at a more comprehensive understanding of the factors which influence and direct processes of socio-technical change by

[12] The long-range goal of such an undertaking is to foster a better understanding of technological change both by bringing into play the sorts of conceptual and theoretical resources that may help us to think differently about it and by concretely demonstrating their utility through an analysis that will expose some of the forces that shape the development of the Internet, and how these forces simultaneously re-shaped society at the same time.

overcoming the opposition between endogenous and exogenous approaches to the explanation of such change.[13] According to the first approach, also known as the *internalist* tradition, trajectories of technological development and directions of innovation are largely conditioned by intrinsic factors like the state of scientific knowledge and technological capacity. Changes in technological design, proposals for the further development of techno-social systems, and the directions pursued in terms of exploration and innovation are tied to logics of scientific discovery and to the exigencies of engineering knowledge. The second approach, also know as the *contextualist* position, relies on extrinsic factors to explain trajectories of technological development (Staudenmaier 1985:18). Through this lens, the problematization of child security and the processes whereby it is subject to solution would be largely explicable in terms of larger structural and systemic forces like public expectations, economic demand, or the exigencies of the prevailing government apparatus.

My purpose, in contrast to these two traditions, will be to chart a diacritical analysis which attends to the role played by both endogenous *and* exogenous factors/forces. To be more precise, the investigation will describe the role that endogenous *and* exogenous factors/forces played in the processes by which the safety of children in cyberspace came to be regarded as a problem in the first place, and it will consider the role played by these same exogenous and

---

[13] A good survey of both traditions, and the conditions which contributed to the rise and fall of each is provided by Staudenmaier's 'Technology's Storytellers: Reweaving the Human Fabric' Cambridge: The Society for the History of Technology and MIT Press, 1985.

endogenous factors/forces in the subsequent processes of problem solving which ensued and aimed to address the issue.

My aim will be to describe the role that risk logics and neo-liberal rationalities of rule (exogenous considerations) on the one hand, and distinct properties associated with the design character of the Internet (endogenous forces) on the other, played in structuring the emergence of a particular problematic, which I dub the securing-child-safety-in-cyberspace problematic, and to show how this problematic was interpreted in a variety of contexts where problem-solving strategies developed and were adopted to address it. Subsequently I shall describe the processes of problem solving that arose across design, operations, and emplacement contexts in order to explore their impact, importance and implications.

1.1 Scope and Terms of Reference

With respect to scope, the Canadian context over the period of 1992 through to 2005 provides the immediate frame of reference for my examination of some of the key processes associated with the development of the securing-child-safety-in-cyberspace problematic. The second part of the examination, which looks at the securitization processes associated with addressing this issue by creating security solutions of various sorts and by developing structures to govern security in cyberspace, however, extends beyond the Canadian context simply because such socio-technical processes cannot be geographically isolated. Given this stipulation, I have endeavored to try to make sense of the

development of approaches aimed at securing children in cyberspace and of structures aimed at governing such security by locating them against and framing them in relation to the broader backdrop of the rationalities of rule characteristic of neo-liberalism, and in relation to the risk logics which characterize advanced capitalist western democracies.

One further stipulation with respect to scope arises and must be acknowledged. The approach I have adopted to understanding the trajectories of socio-technical development associated with securing the Internet for children can be characterized as 'processual'. According to this approach, cyberspace can be understood as a socio-technical environment whose formation and processes of development are open-ended and ongoing. From this supposition it follows that an analysis of the processes involved in addressing the insecurity of children in cyberspace must be traced across the three contexts and distinct domains in which attempts to respond to and address this insecurity have arisen. To be more precise, attempts to address such insecurity will be examined in contexts of design, in contexts of operation, and in contexts of emplacement.

The key terms of reference in this study are securitization and cyberspace. With respect to the latter, it needs to be emphasized that the main motivations for adopting the approach I have was to call attention to the social processes associated with the definition and development of cyberspace. That much said, however, I subscribe to the general premise that cyberspace resists conventional categories in terms of definition. It certainly does not conform to modernist categories of public or private, although it has, indeed, undergone an extensive

process of privatization, so much so in fact that some authors have described this as an 'invasion of the public by the private' (Barney 2001). However, few would consider cyberspace 'private'. I do not imagine a definitive definition of cyberspace is possible, nor do I think any such definition is necessary for the current investigation. As a provisional measure for the present purposes, I have decided to adhere to a conceptualization of cyberspace that follows the path set out by Shearing and Stenning (1981) in another context (and is elaborated on later by Hermer *et al.* (2003) and Huey (2002)) by identifying it as a communal space. My reliance on the idea that cyberspace is 'communal' in this context does not mean community owned, however, and it is not my intention to imply that collective decision making is the typical form of governance in place, though there are notable exceptions with respect to particular online communities.

Bringing conceptual precision to the term *securitization*, a term I use to describe the dominant strategic approach that has informed and organized attempts to address the insecurity of children in cyberspace, will require substantial theoretical ground work. It will also advance through the empirical analyses offered in the last three chapters of the work. For the time being I should say that by securitization I have in mind a general mode of strategic action which aims to reduce or eliminate risk by addressing and acting upon its conditions of possibility. My use of the concept of securitization is intended to encapsulate and reflect a critical set of changes in the nature of policing and provision of security identified by a number of scholars working in the area (Ericson and Haggerty 1997; Johnston and Shearing 2003; Hermer *et al.* 2004).

Securitization as a logic of strategic action can be distinguished from juridification and regulation (Innes 2003). Juridification involves creating the conditions of possibility necessary to bring judicial power and criminal sanction to bear, particularly by creating the conditions of possibility for the enforcement of the law. Regulation, on the other hand, denotes the utilization of administrative and executive controls conducive to steering at a distance. Securitization, in contrast, is a generalized approach to risk reduction or elimination based on prevention, precaution or direct intervention aimed at acting on risk and its conditions of possibility. The distinction between these three logics is employed at a broad level as a means to organize and orient conceptual thinking about logics and rationalities of strategic action, and not as a hard and fast distinction. I take it as a given that, in the processes of creating conditions conducive to governance, societies make recourse to some combination of these three logics and rationalities in establishing the networks necessary for the 'conduct of conduct'. However, in the current context, my interest is in those forms of action which do not rely upon or primarily refer to the exercise of state power for their efficacy but that aim, instead, to reduce the probability or outright eliminate the possibility of acts deemed to be undesirable of occurring by acting upon and altering the conditions associated with and/or integral to their occurrence.

1.2 Summary of the Argument

The work argues that neo-liberal rationalities and risk logics had a pivotal impact on the development of the Internet, structuring dispositions toward, thinking about, and responses to key questions about safety and security. To be

more precise, the work argues that concerns about the threat that the presence of cyber-predators, pornographers and pedophiles posed to the safety of children in cyberspace prompted a broad process of public problematization in which both news media reporting and market place representations played influential roles and that this process culminated in the formulation of a distinctly neo-liberal, risk inflected 'problematic' which: 1) reframed threats as risks manageable through prevention and precaution; 2) functioned as a call for action across a variety of institutional contexts; and 3) served as a call to arms to a variety of non-state actors. Two broader structurally rooted anxieties clearly contributed to the dissemination of this problematic, investing it with additional potency and increasing its likelihood of uptake: a generalized worry about the welfare of children associated with neo-liberalism, and a deeper anxiety associated with the pace of technological change characteristic of risk societies. After considering two different but complementary explanations of the impact that these structurally rooted sources of anxiety had on the process of problematization, I subsequently consider the problematic that emerged in response, showing how it made room for a wide variety of actors and an extensive range of agencies, describing the diversity of securitization strategies they pursued, and showing how these had the overall effect not only of significantly transforming the character of cyberspace but also impacting upon its future trajectory of development.

The investigation begins by acknowledging that there is no axiom from which we could deduce *a priori* either that children as a population would be

specifically singled out as imperiled by the advent of the Internet[14], or that after having been singled out, attitudes toward their peril would be aggregated, organized, and operationalized in terms of a 'security' problematic. An investigation of the problematization process itself is thus deemed as the first order of business. This part of the work explains why threats to children associated with the advent of the Internet became such a going public concern and eventually prompted a broad society-wide process of problematization. Undoubtedly, as the analysis in Chapter Three shows, representations of such threats in media reports and in market place advertising elevated the issue significantly and made it more susceptible to a wider process of problematization. Two additional and related reasons are explored. First, that the consonance of such concerns with two deeper, structurally rooted, anxieties characteristic of neo-liberal risk societies (Ungar 2001) imbued the perception of such threats with additional potency thereby elevating the likelihood that their existence would become the subject of a general societal problematization. Second and related, that these two structurally distinct sources of anxiety not only came into confluence with one another around worries about threats to children in cyberspace, but actually fused in such a way as to redefine the prevailing sense of the scope and parameters of the issue in question. I will deal with each of these explanations in turn before describing the problematic that ultimately emerged as a result of this process of problematization.

---

[14] Indeed, even the most cursory historical survey shows that social responses to new technologies are varied. More importantly, there is every reason to expect that social responses to the advent of the Internet would have been organized under a different conceptual schema and met by a different order of response at some other point in human history.

In regard to the first explanation, the idea is that worries about children at risk in cyberspace merely resonated with two deeper, structurally rooted, anxieties and that this resonance alone accounts for its eventual uptake and problematization. The first of these two structurally rooted anxieties pertains to neo-liberalism as a form of governance and abiding worries about its' capacity to effectively safeguard the innocence of children. While such forms of government observe a basic belief in the sexual innocence of children, the demands associated with safeguarding such innocence may conflict with their main modalities of governance. To be more precise, while welfarist approaches were predicated on direct intervention strategies, neo-liberal rationalities of rule are characterized by a general withdrawal of the state from socialized forms of intervention and by the corollary emphasis they place on minimal modes of governance that work at a distance (Dean 1999).[15] Where children as a population are concerned, basic neo-liberal commitments are strained and this strain may induce anxieties about child welfare. The nature of this strain can be traced to two sources. First, an ontological tension within liberalism between a

---

[15] This retreat from moral involvement by the state has meant that the burden of responsibility shifts to other institutions (Hacking 2002) and to individuals. Such rationalities typically involve a basic displacement of the work of regulation to other already existing authorities and institutions on the one hand, and in the formation of entirely new entities and regulatory agents organized around and oriented toward risk logics on the other. While I will say more about how this logic applied in the Canadian approach to the Internet subsequently, it is important to indicate that a broadly neo-liberal approach is indicated in so far as the state both declined to play a direct role in regulating content and/or conduct (a contention clearly supported by the decision of the CRTC in this respect) and that it also opted to delegate decisions regarding the future development of the Internet to a non-governmental committee dominated by private sector interests and an orientation aimed at harnessing the technology to serve the engines of economic growth (I am here referring to CANARIE – an arms-length organization created by Industry Canada to oversee the progressive privatization of the Internet backbone in Canada). http://www.canarie.ca/about/index.html.

naturalistic conception of civil society as composed of individuals whose autonomy is basically immutable, and a sociological conception of this same community in terms of which autonomy is an artifact of forms and approaches to government (Hindess 1997). The tension between these two conceptions reaches its most extreme form where providing for and ensuring the welfare of children and youth are at issue. Indeed, while liberal rationalities of rule are otherwise fairly able to manage this tension (whether or not the assumption that individuals are empowered agents responsible for their own choices holds), in the case of children no such concession can be made. Liberalism cannot confer, without contradiction, an assumption of autonomy directly upon the individuals who comprise children as a population. Yet, at the same time, it involves a withdrawal from the very forms of intervention which would allow it to manage the needs associated with their dependency.

The second anxiety can be linked to more general concerns about the form of the Internet itself as a new medium which ostensibly resists juridification to the extent that it may even be ungovernable. The latter sentiment is suggestive of a species of anxiety that is increasingly manifest in what many scholars have come to describe as 'risk societies' (Ungar 2002; Beck 1996; Van Loon 2002). Indeed, according to this line of argument, this species of anxiety derives from a deeper apprehension and ambivalence about the prevailing trajectories of technological progress within modern neo-liberal nation states. More particularly, the manifest public concern emerging in such contexts is that trajectories of technological change may have unintended and endangering

effects, and that these effects may be beyond the ability of humanity to control. As we have already seen, these sorts of apprehensions in relation to cyberspace were likely exacerbated by early assertions by a variety of experts to this effect.[16] According to other commentators, these kinds of claims produce anxieties that are both symptomatic of post-industrial information societies and are particularly characteristic of the risk societies:

> Beck (1992, 1995) subsumes these new sites of social anxiety under the concept of a risk society. While risks are an inevitable consequence of industrialization, Beck claims that the 'side effects' produced by late modernization are a new development. As compared to the recent past (and especially prior to the Second World War), these risks have novel impacts that are: 1) very complex in terms of causation; 2) unpredictable and latent; 3) not limited by time, space, or social class (i.e., globalized); 4) not detectable by our physical senses; and 5) are the result of human decisions. Essentially, the economic gains following from the application of science and technology are increasingly being overshadowed by the unintended production and distribution of 'bads'. These have gone from being unrecognized, to latent, to globalized (Ungar 2001:272).

In Beck's account, the problem involved here is both that the unrelenting pursuit of technological progress in modern societies has created new hazards and risks such that we have seen new possibilities for disaster, danger and risk, and that the general populace residing in such societies is increasingly aware of such realities and thus experiences a general sense of anxiety in relation to this awareness (1992; 1995).

The second explanation considered in accounting for both the prominence and potency of worries about the welfare of children in cyberspace and their uptake in a general process of problematization is that this occurred not simply

---

[16] Indeed, the advent of the Internet was sometimes portrayed as marking a historical point of rupture - in which technology achieved a kind of 'escape velocity' - freeing itself from the shackles of state control and attaining an almost autonomous existence (Kroker 1994).

as a consequence of consonance, or even confluence, but because there was an outright fusion of these formerly separate anxieties such that the very scope and parameters of the problem under apprehension were fundamentally transformed. In fact, when we re-examine narrative practices with this possibility in mind, what we find is not that worries about the proliferation of child pornography, pedophilia and child predators (a neo-liberal anxiety) functioned alongside questions about the very susceptibility of cyberspace to the rule of law (a 'risk society' worry). It is not the case, in other words, that two different sources of anxiety were being staged simultaneously, but rather that one problem was under address. Perhaps the clearest evidence in support of this claim for fusion lies in the fact that the issues came to be designated in hyphenated form: cyber-pedophiles, cyber-child pornography and cyber-predators. Such hyphenation signals that these phenomena were seen as distinct from their offline counter-parts and that specific importance was being accorded to them as 'phenomena' occurring *in* cyberspace.[17]

Two important effects associated with this fusion may have further heightened the likelihood that the issue would become the focus of a broader process of public problematization. First, it significantly expanded prevailing perceptions of the nature and scope of the challenge. Questions of means (or *techne*) came to the foreground as challenges in their own right and the issues of

---

[17] We need not look very far to find some explanation as to why they would be seen as distinct, for cyberspace is constructed in these same discourses as a *unique medium* wherein the efficacy of the rule of law is less than certain. To be clear, the fact that these activities are occurring in cyberspace is a key part of the problem, and not incidental to it, in the self-understanding of the claims makers precisely because of such uncertainties about the efficacy of state power.

appropriate and effective approaches to control became an essential part of the problem. Second, and as a result of the first, a much broader array of actors and agents ended up being implicated and/or responsibilized in the definition and solution to the problem. Rather than a simplistic rehashing or rehearsing of an 'old' problem in which the activities of child pornographers, pedophiles or child predators occupy central stage, what occurred instead, as a result of this shift, was that a whole order of other questions opened up as also in need of address. The parameters of this more expansive conception of the problem significantly surpass questions about how to fight child pornography or pedophile networks, nor even are they limited to questions about how to do so online. Indeed, there are a plethora of new threats on the horizon that include the possibility that children might know more than their parents about the medium the latter are responsible for regulating, that children might be accidentally exposed to illicit or harmful images, that they might fall in with the wrong crowd, and that their innate curiosity might prompt them to behave in ways that would endanger their innocence.

Given this argument with respect to the conditions that contributed to a society-wide process of problematization in response to threats to children in cyberspace and this broad sketch of the character of this problematization, it remains to explain why this problematization produced the particular problematic which I shall heretofore refer to as the 'securing-child-safety-in-cyberspace' problematic[18]. In addressing the formation of this problematic, I identify three

[18] My use of the term problematic throughout this investigation is not meant to be overly precise or specific. However, I think the some of the elements taken from Rose provide a

factors which contributed to the framing and operationalization of the issue in terms of the securing-child-safety-in-cyberspace problematic. First, I argue that one consequence of the expanded conception of the scope and parameters of concerns about child safety was that a much more capacious way of conceptualizing and organizing the issue would be required. It is a question, now, of how to provide for and secure the safety of children 'in cyberspace'. This will require some determination as to both how to protect children from themselves (and especially their innate curiosity), some idea about how parents ought to govern and regulate their children's use of the Internet, and at the broadest level, some conception of the appropriate division of labour between the sundry agencies and authorities with an interest in, or responsibility for, the safety of children in cyberspace.[19] Second, I refer to the structuring effects of risk logics. To be more precise, the growth of a general apprehension about technological complexity has fostered a focus on risk and an orientation toward forms of social organization, predicated on principles of the individualization of risk and an approach to risk reduction informed by philosophies of precaution and prevention[20] (Ewald 1991; Haggerty 2003). Third, I note that neo-liberal societies

---

good gloss: 'a constellation of issues that need to be considered at higher as well as lower scales; have a large social content; interact and intersect with one another' (1974: 148-149).

[19] It follows from this line of argument that early claims making with respect to the issues cannot be treated as just one more public rehearsal of a generalized anxiety about pedophilia, child predators and child pornography. It is necessary rather to recognize and credit the extent to which a distinctive problematization was in the processes of emergence in relation to these activities in cyberspace.

[20] Although I find elements of Beck's argument valuable and compelling, in later sections of this work I shall chart a course that is more consistent with the Foucauldian conception of risk as a form of governmental rationality. For work which has attempted to arrive at a synthesis between these two perspectives, see Ericson and Haggerty (1997).

are generally characterized by a disposition to frame, organize, and respond to issues of risk in terms of security. Indeed, securitization is the preferred mode of response to risk in neo-liberal societies. Because neo-liberal societies are reliant on civil society and the private sector, attempts to manage security often result in an intensification of efforts aimed at 'governing at a distance'. This involves enlisting the aid of proxy entities, which must also be trained. These proxies are typically parents, teachers, librarians and other *in loco parentis* relations.

Given an explanation of the conditions responsible for a society-wide process of problematization in response to the threats to children in cyberspace, and with an account of the formation of the problematic that emerged to respond to it in hand, the work then goes on to argue that sum-total of responses to this problematic can be organized and understood around the broad banner of securitization. Securitization is understood as a strategic mode of response to risk in neo-liberal, advanced capitalist societies that seek to reduce 'insecurities' by acting on their conditions of possibility. While securitization is the dominant strategy adopted, the investigation in the second broad section of the work is dedicated to describing its distinct tactical forms and to showing how these depend upon on the context or action domain under address. In the case of the dangers posed by the circulation of and exposure to child pornography as well as those posed by pedophiles and child predators, we see that securitization strategies are embodied in a variety of tactics that aim to reduce the likelihood of such events actually occurring.

Three tactics are central to securitization as a generalized strategy: embedding, intermediation/intervention, and responsibilization. To be more precise, I shall contend that embedding is the dominant tactic in contexts of design, that preventative intervention is the dominant tactic in contexts of operation, and that responsibilization is the dominant tactic in contexts of emplacement. Finally, the analysis aims to show that it is important to distinguish between the problem solving processes underway in contexts of design, in contexts of operation, and in contexts of emplacement. In particular, it aims to acknowledge that the approaches adopted in order to address the problem in these contexts may reflect not only differing interpretations of its essential nature, character, and/or extent, but also reflect differing convictions about the costs and benefits associated with adopting different approaches to its address, differing convictions with respect to the question of the corrigibility of the problem more generally, and finally, differing perceptions of the agents or authorities who hold a share in the responsibility for addressing it.

Moreover, consistent with the individualization of risk characteristic of neo-liberal rationalities of rule, what we find is that many of the securitization strategies that have evolved to address threats to child safety operate at the furthest point downstream, empowering, indeed exhorting, agents in contexts of emplacement to follow a 'do-it-yourself' approach to security. This is accomplished both by redesigning the operating environment (through embedding) as well as altering the conditions of access to cyberspace as an environment by para-technical means.

1.3 Design, Methodology and Data

With respect to design, methodology and the collection of data, the investigation was conceived as one which would transverse a number of contexts. As such, a diversity of data sources has been employed, depending upon the substantive issues and constellation of relations under investigation. In so far as the types of data employed in each case were varied, it seemed important that I have recourse to a range of analytic approaches and/or methodologies. While this strategy is generally consistent with the notion of triangulation extant in the theoretical literature regarding questions of methodology (Olson 2004), I have not here deemed it necessary to enter into a full blown review of this literature. Rather, the data employed in each step of the analysis, and the analytical approaches and methodologies used to make sense of them are discussed in more detail as they arise. In what follows then, I provide a brief overview of the research design.

The broad character of the research questions under investigation presented several challenges in terms of the development of a serviceable research design. Three issues were identified as paramount in this respect. *First*, the design would need to allow for an exploration of the various claims makers and kinds of defining claims involved in the development of the securing-child-safety-in-cyberspace problematic in the first place, and it would have to provide a means with which to make links between these defining processes and their subsequent interpretation in action contexts devoted to problem-solving. *Second*, since no specific context of problem solving could be identified, to the extent that

it was clear that these were inherently 'trans-territorial' in nature, the approach adopted to facilitate their analysis centered around the designation of distinct 'action domains' rather than relying on some set of physical coordinates associated with Canada as a nation state. *Finally*, the research design would need to acknowledge that processes of problem solving and the development of tactics for securitization were not *co-synchronous* across these domains. Rather, it was important to acknowledge and allow for the fact that the pace and intensity of mobilization aimed at problem solving varied according to differing domains. For example, the processes associated with the development of coordinated state initiated intervention strategies like the Virtual Crime Task Force occurred much later in the overall processes associated with securitization than did the development of embedded approaches to self-regulation associated with filtering systems. For this reason it was necessary to employ a more elastic frame of temporal reference in relation to each domain. To be more precise, data were collected with reference to the following times frames in relation to each context (Table 1.0).

Action Domain	**Tactical Approach**	**Time Frame**
Design Contexts	Embedding	1995-2003
Operations Contexts	Preventative Intervention	1995-2005
Emplacement Contexts	Responsibilization	1995-2003

Table 1.0 Data Sets Relative to Domains Under Investigation

For the purposes of conceptualizing the research design in relation to the collection and analysis of data, my aim was to conjoin the theoretical framework provided by the social construction of problems approach with more specific models developed in the social construction of technology tradition in order to address processes associated with the interpretation of problems and their address across a variety of action contexts.

Firstly, in terms of conceptualizing and analyzing the processes of claims making leading to the formulation of the securing-child-safety-in-cyberspace problematic it should be noted that a full-blown quantitative content analysis was deemed unnecessary for the purposes of the dissertation and was eschewed in favour of a repeated immersion in the texts for the purpose of a qualitative analysis that discerned the major themes. In preparing the textual analysis several modifications were necessary in terms of design. In so far as one of the emerging themes suggested by the initial analysis of the data was the extent to which neo-liberal commitments had a structuring effect both on the content of claims making and on the formulation of the problematic that eventually ensued, I thought it was necessary to augment the model articulated by Spector and Kitsuse (1995) by adding some reference to the role played by structural factors in the constructionist understanding of social problems. To be more precise, in order to foreground considerations that might otherwise remain tacitly in the background and afford their influence more direct specification I have endeavored to call attention to the structural context in which claims making occurs. Attaching this caveat is decisive in so far as risk logics and neo-

governmental rationalities form the broad backdrop against which specific claims about the dangers and threats to children in cyberspace are framed and materialize as such.

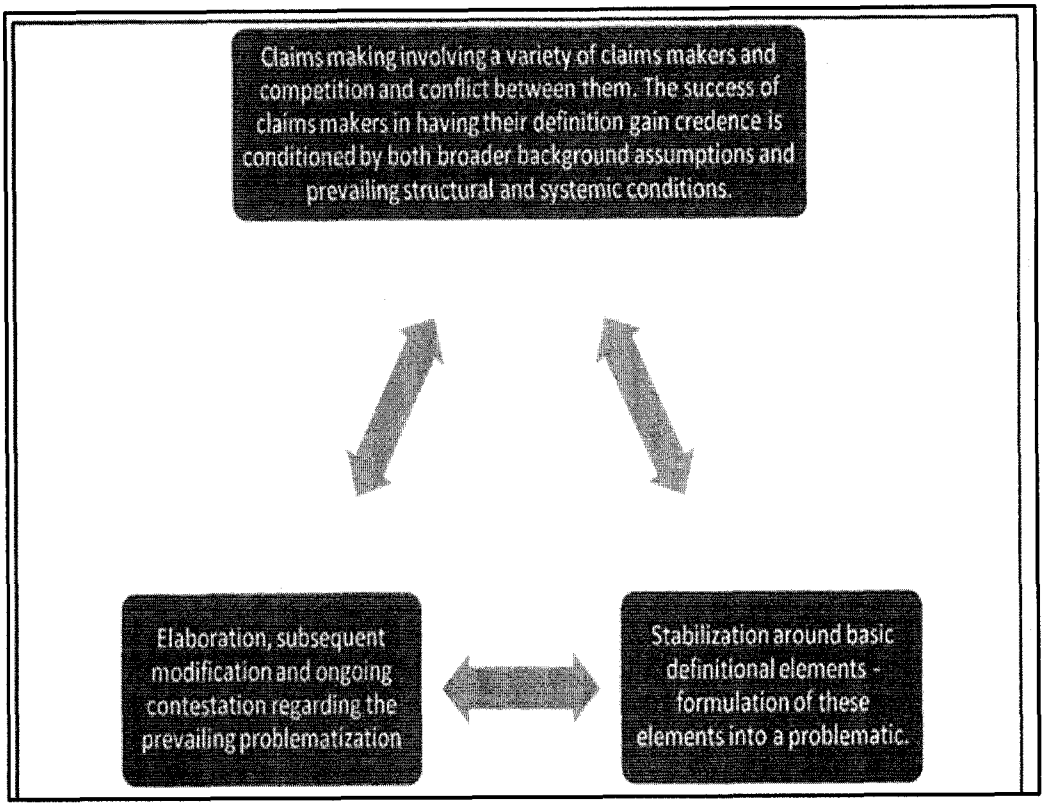

Figure 1: Reconceptualization of the Problematization Process

The puzzle that eventually emerged as salient as a result of examining the content of claims making and the relative success of claim makers was why the definition of the problem as centrally and essentially one of 'securing-the-safety-of-children-in-cyberspace' repeatedly recur and eventually came to be recognized and accepted, serving subsequently as the basis for both action and problem-solving strategizing. After all, any number of other problematizations might have emerged and gained recognition instead. For example, the problem

could well have been defined as one of keeping any and all material which might be harmful to children out of cyberspace completely. It may also have been defined as one of keeping children out of cyberspace completely, as one of needing to create a centralized agency mandated to vet and censor the content of cyberspace, and/or as one of needing to create an entirely different 'for children only' cyberspace. It might also have precipitated a full-scale cyber-war on child predators, child pornographers and their 'ilk'. Positioning this puzzle in relation to the theoretical literature regarding the structure of neo-liberal rationalities of rule, their disposition toward self-regulatory solutions and their deployment of risk in the service of responsibilization, suggested some initial hunches (rather than hypotheses) and eventually opened onto a larger question about the character of the challenges confronted by neo-liberal societies in their ongoing attempts to govern the security and safety of children.

1.4 Contributions of the Work

Two insights into the state and shortcomings of current social science research related to technology were influential in the conception and design of this study. First, that the social sciences have produced a great deal of research that treats technology as a causal force and investigates its impact on social cognition, conditions, relations and structures, but also that such literatures presuppose some sort of meaningful separation between technology and society, and that the technological form is causal in this relationship. The second, aligned with the first, is a predominant tendency within the aforementioned literatures to

foreground and focus on the processes of cultural lag (Ogburn 1964) associated with adapting to the presence of a given technology. The cultural lag thesis has almost become proverbial in much contemporary thinking, and its effect may be to deny the extent to which trajectories of technological development are determined by human values.

Given these considerations, the contribution aimed at by the work was to sketch a way forward for further studies of cyberspace by developing a framework within which to conceptualize its ongoing processes of construction in socio-technical terms, and to articulate a robust set of conceptual and critical tools serviceable for such studies. To do this, the thesis sought to bring the Social Construction of Technology (SCOT) approach into closer proximity with both the social problems school and literatures on risk and security within criminology. Its contribution was to draw upon and draw out the products of this union in order to augment current theoretical approaches to thinking about cyberspace by describing a much broader arc of its processes of social organization and showing how these were explicable in terms of larger systems logics and structuring forces.

Several secondary contributions are also noteworthy. First, the work underscores the continuing importance in the social sciences of Foucault's contention that we have not yet 'cut off the head of the King', both by showing that criminological research on cyberspace has been overwhelmingly state-centric and that it has been predominantly negative, focusing on the prohibitive power of law rather than positive forms of power and their impact on the

organization of cyberspace. In this context, the analyses will show that, in both thrust and direction, the project of securing the safety of children in cyberspace has not principally focused on enforcing the law. Indeed, such ideations reflect an antiquated understanding of the nature of social control, and also tend to perpetuate a misconception about the nature of policing. Second, and related, the thesis aims to support and expand upon the current re-conceptualization underway with respect to policing and security, by exploring the networked nature and nodal structure of the players involved in securitizing cyberspace.

1.5 Caveats and Qualifications

First, for the purposes of this investigation I adopt what can be characterized as an agnostic position with respect to the question of whether and to what extent children are actually 'at risk' in cyberspace. This is not because I am skeptical or incredulous, but because the research as designed cannot shed light on such questions. What is under investigation are the processes by which children were defined as imperiled by (and in need of protection within) cyberspace, how this problematic formed and was taken up in specific action contexts, the problem solving actions which emerged in response to it, and how the adoption of these strategies transformed the Internet. Hence, in regard to the processes associated with the development of child-safety-in-cyberspace as a problematic, the work explores both the various claims involved in the processes of defining cyberspace as unsafe for children and asks how these claims were subject to assessment, taken up and acted upon.

Second, and related, in the context of this investigation it is not my contention that cyberspace was once an unsafe and insecure place but that now, having been subject to processes of securitization, it is secure and safe for children. In saying so I do not mean to imply that securitization is a process that produces no products, or that the effect of these processes has no bearing on the relative security or insecurity of children in cyberspace. Just as my purpose is *not to judge the validity of claims about insecurity, it is also not to make any* judgments about the efficacy of securitization strategies. Rather, my contribution consists in insisting that we need to acknowledge how broad sets of concerns about the dangers and threats to children in cyberspace came to find formulation in terms of the 'child-safety-in-cyberspace' problematic and how this problematic impacted on the overall processes associated with the ongoing socio-technical construction of the Internet.

Third, and related, security in and of itself eludes and cannot be subject to objective definition. It is a goal that always exceeds our grasp, not an end state that can be reached. In this context Ericson has argued we can never have too much security (2006).

Fourth, the research findings raise a variety of questions about the implications associated with adopting approaches to criminal justice based on risk versus those grounded in a commitment to punishment. To be more precise, my investigation shows that, in several cases, securitization strategies show little or no interest in bringing prospective perpetrators to justice. While I am aware that there is a larger literature and debate underway within criminology around

this question, particularly as it bears on the larger issue of 'justice', I do not intend to delve into these issues here.

Fifth, while the behaviors I am investigating are those associated with defining the Internet as an 'insecure' space for children and attempting to make it more secure, it should be stipulated that the meaning of insecurity and security in these contexts is neither unambiguous nor uniform. Indeed, a key purpose of the analysis is to expose the way that insecurity is constructed by various parties and to link these constructions to the processes of problem-solving associated with addressing them. It should also be stipulated, however, that there are a great many discourses at play in relation to security issues. This thesis does not deal with insecurities associated with the desire to utilize the Internet for electronic commerce, nor does it aim to investigate the processes involved in attempting to secure the Internet against viral attacks, spyware, and/or malware. It does not, for that matter attempt to deal with any issues around the securing of data on the Internet for the purposes of storage and retrieval. All of these are perfectly legitimate issues for investigation, and though they may be touched upon here, the analysis of any of these issues is left for another investigation.

1.6 Overview of the work by Chapter

In Chapter Two I lay the theoretical groundwork and establish some basic conceptual scaffolding. The chapter is divided into two sections. In the first section I draw upon the Foucauldian notions of eventalization and governmentalization to provide a broad conceptual framework within which to

make sense of the processes associated with the development of the Internet. Subsequently, I introduce Foucault's notion of bio-politics and his analyses of neo-liberal rationalities of rule in order to sketch a broad backdrop against which claims making about the perils that cyberspace presented to children might be understood. More precisely, I describe the transformation from forms of social organization oriented toward social defense into discourses associated with state security, social risk and population. Finally, I locate the claims analyzed in the first empirical chapter in a broadly social constructionist framework and indicate how this will allow for an exploration of the processes associated with the development of the 'securing-child-safety-in-cyberspace' problematic.

Chapter Three links the representations of threats to children in cyberspace found in the newspaper media and extant in marketplace advertising to the broader structuring logics and exigencies of neoliberal risk societies described in Chapter Two. The chapter begins by distancing the analysis being undertaken from the moral panics approach and subsequently sketches out an alternative approach based on the Copenhagen School of security studies. The appeal of this latter approach lies in the fact that it explicitly brackets off questions about the validity of claims made with respect to the existence of threats in order to avoid the conundrum of having to take a position with respect to their ontological reality. With these and several other theoretical preliminaries in place, a specific account of the role these representations played in processes of problematization is offered. I argue that the influence of the latter (structuring logics) can be seen in a general disposition to translate the threats to children

posed by cyber-pedophiles, cyber-pornographers and cyber-predators into risks that are susceptible to management and minimization strategies. I argue that the effect of these structuring forces is seen in the fact that the problematic of securing-child-safety–in-cyberspace became the dominant way of thinking about and approaching these issues. Two features of this problematic are identified as critical; first, that it operationalized the problem as one of security and second, that this had the effect of drawing in a much broader spectrum of actors and of making the imperative actionable across a broader spectrum of contexts. The work then explores the role played by newspaper media in the representation of claims about the nature of threats and dangers to children in cyberspace and contends that the effect of these representations can be conceived in terms of the formation of 'the child-safety-in-cyberspace' problematic. Its purpose is to present a clear account of the processes by which these threats were represented in media and marketing contexts so that (in subsequent chapters) the impact of these representations can be explored in relation to the development of securitizing strategies. The role of expert authority is subsequently considered. The chapter then offers a fledgling account of the processes associated with the translation of threats into dangers and of dangers into risks. The chapter concludes by discussing the end product of these processes of problematization using the metaphor of a virtual 'Rogues Gallery'. This gallery, it contends, serves as a fundamental point of reference and reserve for both the conceptualization and justification of security initiatives, approaches, and strategies.

In Chapter Four, I review, organize and evaluate theoretical approaches to the explanation of trajectories of technological development. Subsequently I map a course that aims to respond to and redress some of the theoretical and conceptual shortcomings in this literature. First, I sketch a backdrop for the current investigation that describes the rise of neo-liberal approaches to government and the emergence of risk as an organizing ethos. Doing so is necessary to understand the way that these larger system logics imbue concrete action contexts with pre-interpretative orientations, and have a steering effect in so far as they privilege securitization strategies in the processes involved in the design, operation and emplacement of a given technological system. Finally, Foucault's analysis of the transition to 'risk' modes of government is linked with the portability of disciplinary apparatuses through an analysis of strategic coupling. In terms of concrete contexts, this work also provides a route through which to analyze the processes of social construction occurring in fields of emplacement. To be more precise, following Foucault's contention that governmentality be conceived as a kind of 'conduct of conduct' which simultaneously 'totalizes and individualizes' provides the basis for a stereoscopic analysis wherein questions of anamato-politics are paralleled at the state level by considerations of bio-politics (Foucault 1981). In the penultimate section of the chapter I turn to and critique the social construction of technology literatures in order to develop an integrated approach to the analysis of processes associated with social construction. While constructivist literatures are shown as helpful on the design end of the continuum, they do not take into account the role of

intermediaries and interveners on the one hand, or contexts of emplacement on the other.[21] Since one of the defining features of cyberspace as a 'virtual reality' is its ineradicable plasticity, it is necessary to account for the fact that the Internet is design all the way down. The chapter concludes by offering a model for the investigation of processes of securitization across the three action domains identified earlier.

Chapter Five examines the development of security imperatives in the context of design. The point of embedding as an approach is that code, architecture, and programs have police 'effects'. They enforce compliance in a way that far surpasses the way that the presence of a police officer at an intersection would. The point is also that these elements are 'designed in', that their design is intentional, that their designers are acting to induce some form of social control, and that the possibilities for resisting such designed in intentions are limited. Rather than describe the overall role security imperatives play across design communities, however, I here focus on the development of filtering software as a paradigmatic form of embedding. I argue that filtering software gives new meaning to the idea of being a moral entrepreneur, and that what we see in this kind of embedding is a kind of privatization of moral judgments.

Chapter Six explores the role played by intermediaries and interveners in securitizing cyberspace. Intermediaries operate in an indirect and often undetectable way in so far as they operate beyond specific contexts of

[21] This interest in and regard for contexts of emplacement can be seen as one which parallels trends within the media studies literature wherein there has been a broad shift away from structural studies which attempted to decode content at the level of signification, toward reception studies which ask how people make sense of and understand television in specific contexts.

emplacement. Their actions may have bearing on individual users, or alternatively, have uniform effects across contexts of emplacement. Interveners, on the other hand, are agents who enter cyberspace as an environment for the purposes of altering behaviour by command, by coercion or by law. Recent scholarship in the area of policing and security has highlighted a number of prominent transformations (Cooley 2004). As conventional, taken-for-granted, distinctions between public space and private property have become blurred and increasingly difficult to define, the jurisdictional purview and division of labor between public police and private security have followed suit; the rise of the neo-liberal state has prompted the delegation of many functions formerly monopolized by the public police to private security and even third sector organizations. Rising demand for security prompted by public fearfulness has further strengthened the development of the private security market. Processes of securitization have transformed the context in which policing occurs. In response to a more general sense of dissatisfaction with 'Statist' connotations associated with classical criminological conceptions of police and policing, and in response to the fragmentation of formerly functional unities that defined policing as a whole activity, some scholars have undertaken to re-operationalize policing questions in relation to the construct of governance (Hermer *et al.* 2004). According to such scholars, in relation to security, we are witnessing the emergence of a second paradigm in which 'security is everybody's business' (Johnson 2003). To this we might add that conceptualizing security is everybody's business too. The analysis in this chapter shows not only that the

emergence of the Internet has given rise to new regulatory agents and parapolice (Rigakos 2002), but also points to the need for a more detailed study of the way that policing strategies and tactics have changed in order to address security in cyberspace.

In Chapter Seven I describe the household as a scene of emplacement and discuss how processes of responsibilization have unfolded in this context of emplacement. My aim is to show that the construction of security in this context can be understood as a consequence of sundry inducements, incitements, and imperatives that emerge from elsewhere, and particularly to argue that the processes associated with emplacing the Internet in the home have had the effect of re-governmentalizing parenting in some very important respects. The analysis in this phase shows that the tension within neo-liberalism between a conception of children as autonomous and as dependent is most evident in this context in so far as parents must constantly choose between two alternative ways of relating to and seeing their children.

In the concluding chapter I summarize the key investigative efforts involved in the work and summarize what has been learned. Subsequently, I discuss some of the strengths and shortcomings of the work. Finally, I look at open questions. Suggestions for further investigation and research are offered in closing.

Chapter Two:
The Social Construction of Cyberspace in the Neo-Liberal Mode

2.0 Introduction

The goal of this work is to understand the way that concerns about the welfare of children online instigated a broad process of securitization that transformed the nature and character of the Internet. In order to do so we must first understand why the issue surfaced in the first place, how it came to be formulated into a problematic, and how that problematic came to be interpreted and acted upon in the action contexts that will be investigated in the second phase of this work. We cannot assume it was simply inevitable that the advent of the Internet would occasion fears for the welfare of children, or that the only logical response to the manifold of threats associated with the presence of pedophiles, pornographers and predators in cyberspace would be organized and operationalized under the construct of security. Instead, we must investigate why this particular problematic, which is distinctly defensive in so far as it has the effect of focusing effort and attention upon safeguarding potential victims and cyber-proofing vulnerable populations (rather than detecting and apprehending offenders), formed in the first place. In order to answer this question we must first investigate how these threats and the dangers they posed to children were narrated, and try to understand such narration in relation to the larger socio-historical context out of which they emerged.

Locating claims and processes of claims making in their proper socio-historical context presupposes considerable theoretical groundwork and

conceptual scaffolding. The first three sections of this chapter are devoted to this end. In the first section of this chapter I deploy the concept of eventalization (Foucault 1981) in order to mark the emergence of cyberspace as a distinct and historically specific 'event-moment'. Subsequently, I introduce Foucault's notion of governmentalization in order to call attention to the sundry processes of governmentalization associated with the social construction of cyberspace. My aim in doing so is to show that the emergence of cyberspace must be conceptualized as an ongoing accomplishment at the level of social construction, and that this accomplishment needs to be understood as the ongoing outcome of a variety of socio-technical processes and practices. In the second section of this chapter I draw further upon Foucault's corpus in describing some of the background characteristics of neo-liberal rationalities of rule and risk logics in order to locate the kinds of claims made in the processes leading to the formation of the securing-child-safety-in-cyberspace problematic against a broader socio-historical backdrop.

2.1 The Historical Event Moment of Division

> We should refrain from imagining that the events that unfold over the course of our times are somehow definitive and/or epoch defining; but we must nonetheless have the courage to interrogate and explore the multiple and variegated facets that mark our present – giving it specificity, and particularity (Foucault 1991:75).

As a historian, Foucault was deeply suspicious of the 'retreat into the present' associated with the grand theoretical meta-narratives of Marxism and to a lesser extent structural functionalism. But in the above admonition we have

more. Foucault is entreating us to avoid both the fallacy of 'presentism' that cuts us off from our past by inducing us to imagine that our time is somehow unlike any other in human history, and the fallacy of 'historicity', which denies the possibility of novelty in our time by treating all points in time as essentially the same.

Foucault's injunction is particularly propitious in the current context, for no analysis of the character and kinds of claims making involved in the formulation of the securing-child-safety-in-cyberspace problematic can proceed without first acknowledging - as defining - the historical 'event moment' which is the condition of possibility for the emergence of the problem as such. I am, of course, referring to the moment at which the idea of a division between virtual reality and reality[22] emerges, as well as the subsequent processes through which the division between these two domains eventually stabilizes.[23] Foucault utilized the notion of the event and a procedure he called eventalization to try to make historical sense out of the emergence of such dualisms without divesting them of their particularity or specificity. Eventalization as a mode of analysis attempts a radical break with other modes of historical research. As an approach to investigation it focuses on the continuities and discontinuities within specific kinds of discursive formations and material relations in order to account for both the field of experience which opens itself up to acting subjects and the constitution and activity of subjects

---

[22] A number of other 'pairs' might also have been used to indicate this division: cyberspace vs. the real world, or the online world vs. the offline world.

[23] In the language of the social construction of technology approach (Biker *et al.* 1987), closure refers to the stabilization of a technology around a particular use or set of uses. Kline and Pinch (1996) have added that technology 'often becomes closed around a dominant form, but that interpretative flexibility may challenge that closure' (Salter 2005).

within that field. For Foucault, such events may include the development of dividing practices described by his genealogies, the development of various forms of utterances as analyzed in his archaeologies, and the agglomeration of both practices and utterances analyzed by his method of problematization. One of the primary characteristics that marks off the procedure of eventalization, however, is the fact that its aim is to make visible among these different event sequences 'a singularity at places where there is a temptation to evoke a historical constant' and to show not only that that there is no law of necessity at work in historical events, but that the outcome of events was not a 'matter of course' (1991:77). For Foucault, the intent of eventalization is not to produce 'a history of knowledge contents nor an analysis of advancing rationalities which rule our society, nor an anthropology of codifications which, without our knowledge, rule our behavior' (1991:76). Rather, Foucault sees eventalization as a theoretic-political strategy designed precisely to perpetrate a breach of such self-evidences. Indeed, eventalization shows that each historical juncture is characterized by a plethora of possibilities and intelligibilities, and perhaps most importantly a 'deficit of necessities' (1991:78).

The advent of the Internet can be considered an 'event-moment' in the Foucauldian sense is so far as it marks the emergence of a new dualism, namely the dualism between virtual reality and reality, or between what happens in cyberspace and what happens in the 'real' world. Any attempt to understand the content of claims making with respect to the dangers posed to children in cyberspace must begin by acknowledging the appearance of this division as the point of origin and condition of possibility for the problematization which

subsequently developed. Moreover, the development of this division must be understood as an achievement, as the ongoing outcome of a society-wide process of social construction through which a 'space', which at one time did not exist at all (either as a technological possibility or imaginary construction), was subject to parallel processes of social and socio-technical construction that included defining it as somehow distinct or separate from physical space, and investing it with particular properties, powers and potentialities[24].

As an event of rather sweeping sociological significance, the development of the division between virtual reality and reality cannot be taken for granted or assumed as unproblematic. Rather, the emergence and stabilization of this dualism through practices which involve treating the two domains as distinct is something that must be explained. This is so for two reasons. First, only by examining and coming to understand the basic nature of the conceptual claims which underlie and anchor this division can we hope to gain any insight into the distinct nature of the challenge the advent of cyberspace was perceived to pose to traditional means and measures of governance. Put differently, it is only by way of an examination of the content of discourses which define cyberspace as being different than, or even as standing in opposition to, real space, that we will find the key and determining properties which form the foundation for the

---

[24] We see here the development of a corresponding set of dividing practices, not simply at the level of ideation or discourse, but at the level of law, policing, and politics. A set of dividing practices at the level of both social organization and social practice that are predicated on the presupposition that the two domains are relatively distinct. In other words, what we have here is a dividing practice of a character that is, at least in some ways, not unlike the division between madness and reason. Just as Foucault called attention to the historical constitution of madness in such a way as to foreground the finitude of the concept and its historicity, it is important to attend to the historical processes associated with the emergence and stabilization of cyberspace.

particular problematization that developed in relation to its governance. Second, only by understanding the broader processes associated with the stabilization of the division between cyberspace and real space can we gain insight into the nature of the tasks associated with solving the problem of the insecurity of children in cyberspace.

The aim of this thesis, of course, is not to investigate all of the processes associated with the social construction of cyberspace, but only that subset of processes associated with the social construction of cyberspace as a place that is not safe for children and the parallel, though not necessarily co-synchronous, processes by which a variety of actors, agencies and institutions organized themselves and endeavored to alter the character of the Internet in order address this insecurity.

2.2 Stabilization through Governmentalization

With some minor modifications, Foucault's concept of governmentalization provides an appropriately capacious conceptual framework through which to try to make sense of the sundry and variegated processes associated with the social construction of cyberspace. Foucault used the term governmentalization to refer to a specific set of processes in relation to the state. In his conception, governmentalization is a 'productive' process which proceeds first by conceptualizing and attempting to define spaces and populations, and subsequently aims to order and organize them in such a way as to render them susceptible to projects and practices of governance. The term thus refers to the

processes of creating conditions conducive to the emergence of self-organizing, self-reliant networks of governance and not to the networks of governance themselves. Foucault used the term governmentalization to describe the processes whereby the state undertook to strengthen itself and increase civic security (Foucault 1991).

I want to use the term even more broadly than Foucault intended, to designate the processes whereby a number of actors, agents and interests were enlisted in the collective project of conceptualizing and attempting to define both cyberspace (its existing and potential uses) and the processes whereby these actors, agents, and interests were enrolled in efforts aimed at envisioning 'order' in cyberspace and thus in attempting to organize it in such a way as to render it susceptible to projects and practices of governance.[25] It seems to me that, not unlike the lands and territories described by Foucault, the emergence and early history of the development of the Internet can be conceived in terms of a process of governmentalization. This process encompassed a wide range of legal, political, economic, social and cultural actors, involved the mobilization of a variety of forces, and required the expenditure of a vast and diverse array of resources. It meant a veritable re-visioning of existing legal, economic, political, social, and cultural conditions conducive to the emergence of self-organizing, self-reliant networks of governance and precipitated a concomitant redefinition of notions of citizenship, sense of purpose, national aspirations, and visions of the future.

---

[25] Though, of course, these actors were by no means bound by a common agreement about the aims or objectives of that project.

What was involved in this process? The mobilization of expert resources, the formation of panels, and the assembly of working groups and committees to determine its powers and potentialities. The identification and resolution of jurisdictional questions. The delegation and division of responsibilities and the responsibilization of populations and spaces. The allocation of resources and formation of policy frameworks. The constitution and consolidation of knowledge about the nature of the space and system, the assessment of risk with respect to its dangers, and the identification, measurement, qualification and quantification of these risks. The constitution and operationalization of new classes of deviants, of criminal acts and criminals. The identification of vulnerable segments of the population and the development of processes, procedures, mechanisms and tools with which to protect these populations. The development and elaboration of strategies aimed at public education about new economic opportunities and the formulation of policies to promote commercial development.

This process of governmentalization, which encompassed a wide variety of social, economic, political, and cultural actors, and which mobilized a vast and diverse array of organizational resources, had as its byproduct the formation of new species of knowledge about cyberspace and its populations, the development of new orders of experts, and the rise of new classes of regulatory agents. Moreover, while cyberspace was both the subject and object of these processes of governmentalization, the state was neither the prime mover nor the primary stakeholder. Rather, these processes of construction were highly complex and multifarious, and cannot be traced to one plenipotentiary agent,

actor or institution. Indeed, to the extent that modern forms of 'governance' rely on a diffusion of power, this diffusion was informed by a more general orientation toward risk, civic strength and a broader set of bio-political imperatives. In the case of modern neo-liberal societies these processes of social construction can be traced to the organizing role that risk logics play in governing, and to the role neo-liberal rationalities play in enabling and supporting the development of governance oriented actions both civil society and the mechanisms of the

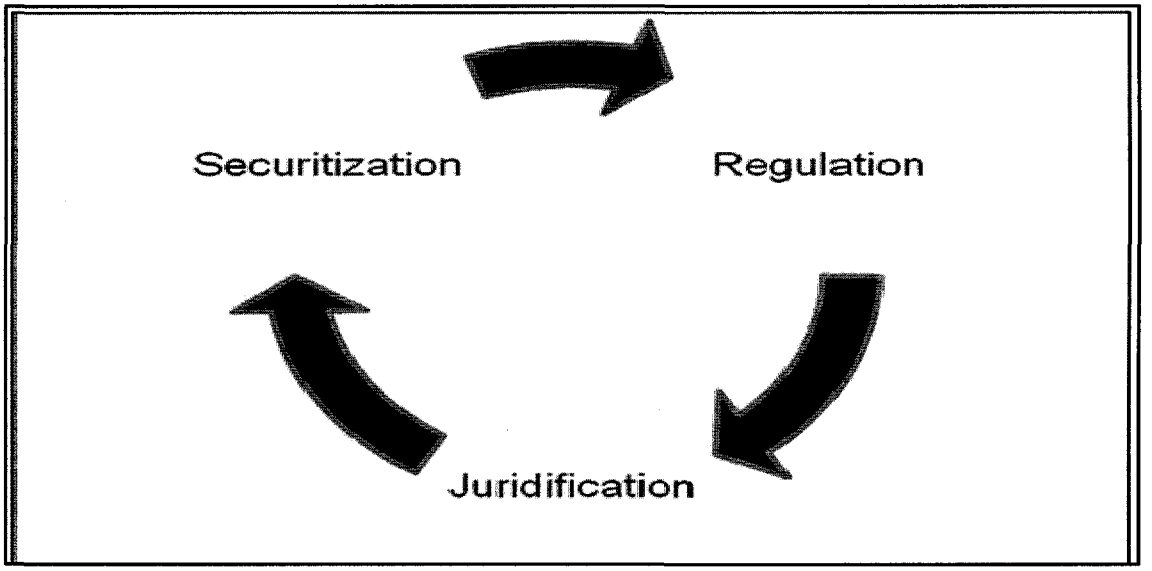

Figure 2: Sub-processes of Governmentalization

marketplace. It is in and through these positive processes, many of which may appear mundane and hence typically operate below the threshold of public perception, and of which the activities of the state formed only a small and often peripheral part, that the social construction of cyberspace has both proceeded and continues to proceed.

While this notion of governmentalization provides a good overall framework within which to conceptualize the sundry and variegated processes

associated with the social construction of cyberspace, a full and unabridged account of the governmentalization of cyberspace, if any such thing is actually possible, is neither needed nor intended here. What I want to propose instead is that, for the purposes of analyses, such governmentalization can be conceived as the ongoing outcome of three distinct but interrelated subsidiary imperatives and their associated logics of operationalization: juridification, regulation, and securitization. Under the imperative of juridification, cyberspace has been progressively subject to processes of legal definition and brought under the umbrella of jurisprudence. Under the imperative of regulation, cyberspace has been subject to the larger administrative rationalities characteristic of neo-liberalism. And, under the imperative of securitization, cyberspace has been subject to a series of strategies aimed at prevention, preemptive intervention and responsibilization.

2.3 Contextualizing Claims Making and Processes of Problematization

In this section, the initial form of the idea of 'governmentalization' is explored, modified, and developed to reflect neo-liberal realities and to render it useful for the conceptualization of the Internet's processes of construction and development. I begin by sketching an argument that links the emergence of the Internet to the exigencies and *modus operandi* of bio-power. To do so, I first describe and discuss some of the broader sets of forces that stretch across the horizon of modernity and describe the structural and organizational impact they have had on social, political, and economic conditions in the modern age. Only

then, after we have some sense of the deep and abiding way that these forces have shaped our present, will it be possible to examine both the emergence of the Internet and the particular processes of problematization that emerged in relation to its rule in a proper light.

For Foucault, the threshold of modernity is marked by the emergence of what he termed the 'age of bio-power'. Two poles of political intervention emerged, together constituting a 'great bipolar technology' of power over life (Foucault 1991). The first centered on the 'body as a machine'; an 'anatomo-politics' aimed to extort forces and optimize capabilities. The second centered on the 'adjustment of the phenomena of population'; a 'bio-politics' focused on demography (distribution, longevity, procreation), economy (the synchronization of resources and citizens), and social security (the social constitution of contracts and interests), wherein the health and well-being of the *civitas* became a 'general objective of policy' and domain of investment. Foucault argues that these powers become efficacious only after a preliminary process of governmentalization.

According to Foucault's account, bio-power comes to prominence through the interaction of systems of knowledge and forms of governmentality. More specifically, politics becomes bio-politics when the state's concern turns to the health and wealth of the population as a measure of state strength. Foucault argues that the efficacy of bio-power derives from a belief in the validity of the network of disciplinary training and systematic surveillance that has developed because of its social benefits. Through their cooperation in the social network, subjects secure material gains: the right to life and security, and a conviction that

threats such as famine, starvation and plague will be overcome.[26] Through his analysis of bio-power, Foucault links the discourses of the human sciences with the various political technologies of the body, and shows how structures of domination and oppression result.

Foucault argues that the practice of documentation is critical to the genesis of bio-power. As the product of on-going practices of surveillance and examination, documentation provides a record of individual action, but it also presents an opportunity for compilation and collective analysis. Hence, while disciplinary practices constrain behavior to make it more knowable, the documentation of such disciplined behavior allows for the production of new knowledge which presuppose these constraints, creating not only more control, but more importantly, a new order of discourse about norms. Foucault says that the development of such normative knowledge begins with the use of probability and distribution tables which 'enable one to locate the individual within an epistemic field without reducing the individual to the typical' (Foucault 1991:112). As the study of norms advances, he argues, it becomes a vital resource for the analysis of population, and a distinctive type of political rationality emerges which

---

[26] Hence, Foucault states: 'Western man was gradually learning what it meant to be a living species in a living world, to have a body, conditions of existence, probabilities for life, and individual and collective welfare, force that could be modified and a space in which they could be distributed in an optimal manner. For the first time in history, no doubt, biological existence was reflected in political existence; the force of living was no longer an inaccessible substitute that only emerged from time to time, amid the randomness of death and fatality; part of it passed into knowledge's field of control and powers sphere of intervention [...].Outside the western world, famine exists on a greater scale than ever; and the biological risks confronting the species are perhaps greater and certainly more serious than before the birth of micro-biology. But what could be called society's threshold of modernity has been reached when the life of the species is wagered on its own political strategies' (Foucault 1991).

is concerned with the state as an end in itself. This concern is strikingly different from previous political rationalities. Indeed, in the new form of political rationality 'the existence of the state, its power and resources, become the subject matter of the new technical and administrative knowledge' (Rouse 1994:103).

This new rationality contrasts with juridical rationalities in which the exercise of power is linked to the end of justice or natural law. Under these new administrative apparatuses, welfare is still defined by people's needs and their happiness, but the end goal now is to increase state power. In fact, the overall aim of this form of governmentality, Foucault argues, is for the state to increase its control over its inhabitants. The field administrators of these techniques were originally called police. Police become responsible for the control of specific individuals and of the general population as they relate to the state's welfare. Because this task of population management requires a variety of information about the population, environment, and resources, the contribution of the human sciences becomes indispensable. This new administrative knowledge is not concerned with the rights of people, but with people as resources. Moreover, their aim is not to develop a general theory, but to concretely describe the state in order to assess its forces and powers and thereby assist it in operating effectively. Hence, two levels of epistemic analysis and political regulation are linked by the practice of normalizing judgment and the construction of the normal as a field of possible knowledge: bio-power and disciplinary power. Foucault's point is that new kinds of knowledge of human beings come about as a result of

these rationalities.[27] Indeed, as Rouse argues, Foucault suggests that there is a complementary constitution of two levels of knowledge produced by discipline and bio-power respectively. At the disciplinary level, there is a growth of 'systematic knowledge of individuals through connected practices of surveillance, confession and documentation' (1994:106). At the bio-political level, population becomes an issue for exploration and ongoing analysis.

The knowledge produced by the human sciences is linked to the broader project of individualizing and totalizing population management necessary to sustain specific political rationalities. Since these projects result in a particular regime of truth, it is now necessary to indicate why these power/knowledge relations have oppressive consequences. Foucault shows that the knowledge produced by these politico-epistemic formations is predicated on statistical and categorical ascriptions of normativity and an essentializing logic of identity. However, his more specific claim is that with the dissemination of disciplinary power and the birth of bio-power, a regime of truth arises that teaches subjects to relate to truth in a particular fashion, while effacing and obscuring the way that political projects are implicated in its production. Indeed, according to Foucault, the modern regime of truth incites subjects to seek truth out through a rigorous hermeneutics of the self while at the same time concealing or denying the degree to which these categorical and normative forms of self-understanding are not

---

[27] These 'political-epistemic practices' constitute new kinds of objects for there to be knowledge about: 'biographical unities like delinquency, homosexuality, hyperactivity; developmental structures such as reading grade levels or appropriate age group attainments; significant distributions such as family history of heart disease, low income'. These practices produced new kinds of human subjects, but they also produced 'new kinds of knowledge along with new objects to know and new modalities of power' (Rouse 1994:98).

transparent, but rather, are implicated and enmeshed in a regime of rationality that has as its aim the management and control of populations.

Whereas power once operated through the sovereign by making a spectacle of itself, as it becomes disciplinary it increasingly operates by making its target more visible and audible.[28] Disciplinary power contrasts with repressive force. Whereas the latter works by coercion and constraint, the former reconstitutes subjectivity by generating new attitudes, actions, desires, and ultimately, new kinds of people.[29] Foucault argues that there are two stages in the development and dissemination of disciplinary power. Initially established and refined in specific institutional contexts, disciplinary techniques were used to neutralize the 'dangerous classes' by increasing their productivity and utility. Subsequently, however, as they were disseminated throughout the whole social body, these disciplinary practices and knowledge gave rise to a new order of discourse about norms and a new political rationality that has 'population' as its object.[30] Foucault calls this new form of power/knowledge 'bio-power'.

---

[28] With respect to visibility, Foucault shows us that surveillance operates anonymously, in a subtle, continuous, and hierarchical fashion. With respect to audibility, examination and the interview are the predominant forms of elicitation.

[29] Discipline derives from and is developed through applied knowledge and institutional practices. As 'a political anatomy of detail, it is a micro physics of power that analyses and reassembles specific behaviors, gestures and movements of the individual through repetitive terrain and detailed scrutiny from the standard point of political control' (Foucault 1979:86). Discipline is achieved by 'reordering space and time' (Foucault 1979:43). It is exercised through hierarchical observation in which space is constructed and individuals are located in a manner that facilitates surveillance between them. Disciplinary institutions are predicated on the idea that individual behavior should be isolatable and observable. This organization enables full control of individual activity.

[30] Foucault thus argues that the super-ordinance of the norm transcends judicial law and signals the apex of the disciplinary society. Obedience to the norm is taught by disciplinary institutions through the mechanisms of normalization. As it disperses throughout society, however, it finds expression in a vast complex of regulations, classifications, distributions, and other techniques of surveillance.

The key point for Foucault with respect to these processes of normalization is that there is circularity between disciplinary practices and knowledge. Practices of discipline are derived from knowledges that are themselves products of prior disciplinary practices. In the long term, regularities in disciplined activity give rise to norms of behavior that are natural precisely because they become habitual. Correct behavior thus becomes normal behavior. The system of punishment corrects deviation and enforces normativity. Normalization thus achieves formal equality by judging people by the same standards while at the same time individuating them in terms of this standard. Foucault cites the examination as a technique that combines surveillance, control and differentiation. Examination makes the mind into an object of knowledge and embeds the individual in the field of documentation. Foucault argues that panopticism epitomizes the disciplinary regime because it generates a regime of permanent surveillance, the effect of which is to generate general forms of oculocentric consciousness that assure the automatic functioning of power (1979:215).

2.4 Neo-liberal Commitments and Risk Rationalities

In making sense of the transition from an analysis which focuses on disciplinary power to one which focuses on bio-power and governmentality, I want to draw upon Dean's extensive adumbration of these issues. Governmentality broadly understood refers to the mentalities of rule characteristic of different eras such as: mercantilism, cameralism, liberalism and

social welfarism. Dean takes his lead from Foucault's commitment to nominalism in relation to the modalities characteristic of such governmentalities. Consequently, he argues that the logic of risk ought to be understood as a way of ordering reality in neo-liberal societies. Or, to be more precise, 'risk is a way of representing events so that they might be made governable in particular ways' (Dean 1999:131). It is thus one component of a variety of different 'forms of calculative rationality for governing the conduct of individuals, collectivities and populations' (Dean 1999:131)

Contrary to Beck, who thinks of risk as a developmental phase which is essentially ontological in character, Foucault sees risk as a key constellation in the overall apparatus of governance that can be better understood as 'a component of assemblages of practices, techniques and rationalities concerned with how we govern'[31] (Dean 1999:133). It follows therefore that risk modalities represent a particular species of calculative rationality, one which 'is tethered to assorted techniques for the regulation, management and shaping of human conduct in the service of specific ends or means' (Dean 1999:134). This conception of risk is critical in so far as it means that the very notions of risk become intelligible through specific forms of representation that render reality in such a way as to make it amenable to types of action and intervention.

---

[31] Dean argues that Beck's approach rests on 3 assumptions: 'First, the totalizing assumption that risk should be approached within the narrative of the modernization process that brings about the risk society. Second, the assumption of uniformity of risk has the effect of making it possible to make a general and abstract characterization of risk in a given kind of society. And third, the realist assumption that the reason why risk is a feature of quotidian existence in the risk society and a component of individual and collective experience is that risk has increased so much that it has outrun its mechanisms of calculation and control'.

What is critical for the present analysis, grounded as it is in the social construction of technology approach, is that Foucault's conception of the governmentalities characteristic of neo-liberalism foregrounds the fact that there is a general displacement of authority, responsibility, and accountability, and highlights the plurality of practices and rationalities through which governing is accomplished and authority exercised. Dean argues that the privatization of risk or individualization of risk is indicative of the retreat from 'socialized risk management techniques associated with the welfare state and the emergence of new forms of governing in contemporary neo-liberal states' (1999:134).

These notions are central in terms of understanding the consolidation of claims making with respect to dangers and threats to children in cyberspace as a problem of securing their safety. Indeed, this problematization is not one which mandates or singles out the state, but rather reflects the individualizing of risk linked to a form of governing that seeks to govern 'through the responsible and prudential choices of individuals on behalf of themselves and those for whom they feel an emotional bond or affinity' (Dean 1999:134).

Put in terms of the broader way of seeing the Internet, the generalized logic of prudentialism, associated with the individualization of risk, is evident in terms of a general orientation toward self-regulation. In this context, the Canadian state did not adopt the role of a main agent of regulation in terms of conduct or content issues in cyberspace. Rather, it adopted a facilitating role in terms of the economic development of the Internet, opting to privatize ownership on the one hand and to delegate regulatory responsibility on the other. The

approach was one which involved redrawing the boundaries of the state's legal, social, and economic responsibility such that cyberspace was primarily positioned as a phenomena of civil society rather than the state. While this repositioning is a fundamental strategy characteristic of neo-liberal democratic societies, in practice the distinction between the two domains operates as a complex regulatory strategy organizing multiple realms which in practice do not remain separate (Valverde 1998).

2.5 The Tension Between Autonomy and Dependence

One of the defining tensions that emerge out of the larger logics associated with neo-liberal modes appears in relation to the governance of children. As indicated earlier, some have argued that neo-liberal rationalities of governance result in a tension between autonomy and dependence. The challenge arises as a result of the quasi-independent status liberalism assigns to children and is witnessed in two tensions. First, there is the tension between the child as autonomous and the child as in need of protection. Second, there is a tension between perceptions of children as 'at risk' and of the child as potentially threatening (Jackson and Scott 1991). To be more precise, risk logics organize children under the general rubric of a population 'at risk' in so far as they are defined by their vulnerability and innocence; but they also are defined as a potential and valuable resource which must be 'developed' to secure the future prosperity of both the state and the nation.

As alluded to earlier, I prefer to see the issue as one which engenders a dilemma of governance and leaves state forms of government within neo-liberal societies in a paradoxical position in relation to children. On the one hand, they bear a special duty of care given the particular status of children as dependents. On the other hand, they have withdrawn from the means and mechanisms and forms of intervention that would allow them to address and attend to the vulnerability created by this dependence. My argument, more particularly, is that the responsibility for addressing this issue is displaced to other agencies and organizations which operate in an *in loco parentis* fashion.

Valverde's work is instructive here in so far as it may provide an important lead in further investigating how this tension is responded to in neo-liberal societies, and particularly how it has been reflected in terms of the problematization of child safety. To be more specific, she argues:

> There is, in other words, not only a pragmatic but a structural reason why voluntary organizations are essential to moral reform campaigns of whatever political stripe. These organizations cannot be seen as mere pawns of the state engaged in doing the dirty work of the state in puppet like fashion. Voluntary organizations usually have their own agenda and are in some ways in opposition to the state even when they receive their funding from it. The interaction between state and extra-state agencies of moral regulation must be concretely analyzed in order to reveal both the ways in which they reinforce each other and they come into conflict (Valverde 1998).

Further insight along this line of argument is provided by the recent work of Jessica Evans. In her investigation of one community where anti-paedophilia campaigns were underway in the United Kingdom, Evans argues that there is a link between the 'mind of vigilantes' and 'the mind of the state' which makes

communities responsible for crime management. Evans argues that the propensity of neo-liberal governing strategies to delegate such functions as crime management to communities may begin with a mere vigilance movement within these communities, but suggests that there may be a tipping point such that vigilance turns the corner and becomes vigilantism. Evans argues that this is in part due to the fact that it is actually a mistake to understand vigilantism as '*populism's agents*' and that in fact, *neo-liberal rationalities of rule may have the* effect of placing an inordinate burden on communities.

2.6 Summation

The foregoing discussion presented theories which argue that neo-liberal risk societies place significant emphasis on delegating the rowing functions of governance to civil society, while retaining key steering functions. In terms of issues associated with law and order, this has been witnessed in the rise of a general focus on community safety and third sector and volunteer associations 'taking charge' of their communities and organizing themselves to address issues of common concern. These findings are important for our investigation in a number of ways. First, as we shall see in the analysis that follows in the next chapter, the formation of the child-safety-in-cyberspace problematic reflects the extent to which third sector (or civil society agencies and organizations) were prime movers in the process of responding to the issues. Indeed, authorities or experts from agencies working on this subject are frequent sources of expertise in media narratives that address questions about what to do about the safety of

your children in cyberspace. Second, with respect to questions of state involvement where police officials are represented in media narratives regarding the issue, we see that they frequently refer to and construct the problem as one of security.[32]

[32] I think it may be worthwhile to consider whether the emphasis on prevention is not institutionally reflected in the functional specialization within police forces. Media relations is often about presenting the soft side of policing and this means according less emphasis to the job of 'catching the bad guys' (a construct according to which many officers still operate) than about helping communities to be safe.

Chapter Three:

Claims Making and the Formation of a Problematic

3.0 Introduction

As previously indicated, the initial period following the advent of the Internet was characterized by a great deal of controversy around questions of control and regulation. A looming leitmotif during this time was that the Internet's architecture and system of routing could be constituted as 'threatening' in so far as it was difficult to imagine how laws based on geographically defined spaces might be applied, and especially how they might be enforced (Geist 2002).[33] Subsequently, however, such generalized anxiety and hand-wringing gave way to more specific interrogatives. Particular threats became more focal drawing in an assortment of experts, interest groups, and sundry other players. The ensuing processes of specification would single out particular types of content and/or activity on the Internet as threatening and particularly threatening to the welfare of information assets, data, specific populations and/or societal health and well being more generally. And, they addressed particular entities that might use the Internet for disreputable, illegal or illicit purposes. Generally speaking, in these processes, the threat horizon came to be broadly constituted in terms of two types of threats: threats to the functional integrity of the Internet as a system and/or the proprietary information, assets, or data it housed, and threats to specific populations.

[33] It is noteworthy and interesting that, despite uncertainties about the properties of the Internet in relation to the question of regulation and control, debates characterized by claims making of the 'yes' or 'no' kind did not become focal (Winner 1980).

When we examine more closely discourses devoted to children as a specific population in relation to these threats, and discourses associated with children using the Internet, three themes are pronounced. First, that the Internet is a dangerous place for children. Second, that children nonetheless belong on the Internet.[34] Third, that the risks associated with children venturing into cyberspace are not unmanageable. In this chapter I explore these discourses in more depth in order to better understand the kinds of claims made and the role they may have played in the formation of the securing-child-safety-in-cyberspace problematic. To be more precise, I analyze and describe two narrative contexts where the issues associated with child safety in cyberspace found representation. First, I examine the way that media narratives represented threats to children. My investigation here encompasses newspaper articles published between 1992 and 2000. The analysis in the first narrative context is informed by the basic caveat that claims makers are subject to the media filter, and thus my interest is in both how the media represents the situation, and how it positions and represents claims makers in relation to it.

The second context I address is claims making in the market place. I am here interested in the character of claims made by various vendors and retailers of security software and in particular, how these retailers represent threats in

---

[34] A variety of assertions reflect this general sentiment. Two are worthy of particular mention. First, it was frequently asserted that their future depends on their facility with technology. Underlying this concern appears to be a basic recognition that computers have become a pervasive and ubiquitous aspect of everyday life and that the ability to make use of and manipulate information technology is a core and basic life competency. The second more specific assertion was that the educational development of children as young people would be interfered with if they were prevented from accessing information on the Internet. This second sentiment appears to refer more directly to the pedagogical potential of the Internet as a tool that facilitates self-directed learning.

cyberspace, what kinds of qualities and/or characteristics they attribute to cyberspace and to the people who populate it, and the remedies they either explicitly prescribe or implicitly allude to in addressing the issue. Of course, my analysis in this context is informed by the assumption that the claims made in these contexts need to be understood as profit motivated. My data in this case are drawn from the marketing, advertising and packaging material produced by five filtering and blocking companies between the period spanning 1997 to 2002.

The chapter begins by sorting through some conceptual preliminaries in order to address the status of discourse in relation to events. It then links ideations of risk to the governance of children in a neo-liberal context to the interpretation of the materials. This discussion sets the stage for the analysis that follows in so far as it suggests that the representations of threats that appear in both contexts rely upon and refer to larger sets of background assumptions about the nature of childhood, and also that they connect specific risk anxieties to modes of responsibilization which are characteristic of neo-liberal rationalities of rule. In the next section I explore the role of newspaper media and merchants in the representation of threats. Subsequently, I describe the constitution of 'expertise' and discuss the role that 'expert opinion' appears to play in processes of representation. Next, events are identified as crucial in the processes by which threats are embodied and thereby become dangers. I argue that events are integral to the formation of scientific bodies of knowledge and maybe prove pivotal in the conversion of dangers into 'risks'. In concluding the chapter I suggest that an important and ongoing by-product of the practices of

representation associated with these processes of problematization is the constitution of a virtual 'Rogues Gallery'. This gallery, as will be shown in subsequent chapters, serves as a fundamental point of reference and reserve for the conceptualization of security initiatives, and justification of specific approaches and strategies.

3.1 Data and Methodology

As already indicated, my interest in this chapter is in the claims makers and claims making processes associated with the formation of the securing-child-safety-in-cyberspace problematic. The work undertaken in this regard looked at two forums where threats to child safety in cyberspace found representation. In the first context, representations of threats to children were examined as they appeared in media narratives. The data collected here encompasses articles published between 1992 and 2000. Boolean searches were conducted using the *Proquest Database* of Canadian Newsstand Major Dallies. The newspapers included in this database included *The Globe and Mail*, *National Post, St. John's Telegram, Halifax Daily News, Montréal Gazette, Ottawa Citizen, Toronto Star, Regina Leader Post, Edmonton Journal, Vancouver Sun* and the *Victoria Times Colonist*.

The search terms employed in the collection of this data included Internet child safety, Internet child security, child safety cyberspace, child security cyberspace, Internet child pornography, cyberspace child pornography, child predators cyberspace, child predators Internet, Internet pedophilia and pedophilia

cyberspace. The search yielded a full text archive of 287 salient articles. The archive of articles was compiled and subsequently subject to two forms of analysis. A basic textual analysis was conducted which looked for the appearance of specific keywords in relation to the identification of themes. A discourse analysis was also constructed which aimed to understand the ways in which media narratives positioned various actors, agents, organizations, and institutions as 'responsible' in relation to the search terms already specified.

With respect to questions of validity, I was well aware that this approach would suffer from the obvious shortcoming that it would not directly address the representations made by such claims makers, but would rather only address media representations of the representations made by claims makers, and how such representations position and represent the claims made by such claims makers. While this way of proceeding seemed initially to me to be a significant shortcoming, I subsequently decided upon it because it seemed to me that the representation of the claims made by claims makers in the media was likely to prove much more influential in terms of the conception of, and response to, the issue.

The second context of claims making addressed was in the marketplace. The analyses here focused on the character of claims made by various vendors and retailers of security software and in particular, how these retailers represented threats in cyberspace and what kinds of qualities and characteristics they attributed to cyberspace and to the people populating it. The data in this case were drawn from the marketing, advertising and packaging material produced by

five filtering and blocking companies between the years 1997 to 2002. The motivation for an analysis of these materials came directly from Bijker (1999) who suggested that marketing strategies be examined in order to understand how technology is presented as a solution to social problems. The approach to the analysis of these materials was not circumscribed by any commitment to a particular way of making sense of their contents. The focus was not mainly on the claims they made with respect to their products (though some attention to this issue invariably became necessary as a result of subsequent contestation in relation to product claims) but rather on the way that the dangers of cyberspace to children were presented by them, and the way that they functioned to locate or assign responsibility for the protection of children in relation to the existence of these dangers.

3.2 Theoretical and Conceptual Preliminaries

While an investigation of media reporting on threats to children in cyberspace immediately raises the possibility of deploying the moral panics perspective, I have elected not to make recourse to this approach or the conceptual resources it affords. Putting the matter this bluntly way may create the impression that I see studies conducted under the moral panic rubric as essentially alike or that I see the field as monolithic and unchanging. Nothing could be farther from the case. Indeed, with Goode and Ben-Yehuda (1994), I would distinguish between at least three different strands of thought within the

overall field of moral panics studies[35]. Indeed, I want to acknowledge not only that there are important differences[36] between these strands as well as the fact that field of study is a dynamic one: the tools and narratives associated with the being challenged from without (Cornwell and Linders 2002) and being revamped from within (McRobbie and Thornton 1995).

Furthermore, tribute can and ought to be paid for the contribution the perspective has made to our understanding of a diverse variety of phenomena. First of all, it should be noted that the uptake of the perspective has been extremely wide, stretching well beyond sociology and criminology into political science and health (Buchanan et al. 2003), history (Hunt 1997: Davis 1986), anthropology, and economics (Goode and Ben-Yehuda 1994). Furthermore, within the fields of criminology and sociology, the approach has had immense heuristic and probative value, serving as a flashpoint for investigations across a wide spectrum, ranging from flag burning (Welch 2001) to obesity, from designer drugs (Jenkins) to skateboarding (Austin 1998).

With much said by way of preamble, however, I should state that my misgivings with respect to the perspective pertain primarily to the elite engineered approach and are fourfold. First, as a matter of method, I have

---

[35] The first, identified with Stan Cohen (the founder of the tradition) they label as the 'interest group' strand which emphasizes the roles played by the media and interest groups, and assigns primacy of place to 'folk devils' of various sorts who are effectively scapegoats made to bear the blame for various forms of strain and ambiguity created by social change (Hunt 1997). The second strand, dubbed the 'elite engineered' approach is largely associated with the work of Stuart Hall (1978) and postulates that moral panics are fabricated by elites for the purposes of social control and manipulation. The third, lesser known strand, they label the 'grassroots perspective' and associate it with the criminological realism of Young and Lea (1993). This last strand looks almost to be the mirror image of the 'elite engineered' approach in so far as it inverts the implication of panic in the name of realism. In other words, moral uproar and discourse may be a response to real existing social conditions.

[36] These differences are particularly important because, as I will indicate subsequently, it is the second 'elite engineered' approach that I find most troublesome.

already indicated that the investigation undertaken here is not one which will afford any insight into the relationship between the 'representation' of threats and their 'actual ontological existence'. In this context I worry that studies in the tradition of moral panics research may sometimes be misinterpreted as demonstrating that the representations made by sets of social actors regarding the existence of a given social condition or circumstance are not actually reflective of 'real' realties and thus that social responses to such representations are also irrational. While there can be little doubt that media representations sometimes fuel over-reactions and excessive anxiety and that in other cases they may ignite hysteria, a warrant to legitimize such judgments would require some method for measuring the relationship between 'reality' and its representation (Hunt 1997).Second, I find myself persuaded by the arguments presented by Arnold Hunt regarding the fate and foibles associated with media uptake of the moral panic concept and its uses of it[37]; and third, in a related way and perhaps as a consequence of this media manipulation, I worry that the concept has come to suffer from what Northrop Frye described (in another context) as 'the psychology of the rumour' – or the immediate association one makes on the basis of an intuition between one's already pre-existing ideas and a concept or idea that seems to capture and organize these ideas. Indeed, it seems to me that more often than not the concept of moral panic is received and interpreted as one which denotes calculated conspiratorial behaviour by elites and that the

[37] In Hunt's work we find a comprehensive survey of the abuse of the term by the media over the period of 1972 to 2007. His analysis describes the peregrinations of the concept and calls into question its usefulness for a variety of reasons. Not the least of these consists in the recurring tendency to misinterpret and misunderstand Cohen's original use of the term and the analysis he developed based upon it.

effect of such easy assimilation and cavalier employment is to extinguish rather than fuel further thought and analysis. The fourth and final reservation I have with respect to the elite engineered approach stems largely from my sympathies with Foucault's critique of oversimplified conceptions of the nature and character of power, and particularly with his insistence on complicating its analysis so as to reveal the extent to which it is dispersed, fragmentary and fluid. This seems to me to be particularly a propos in neo-liberal risk societies wherein it is very difficult to designate a single agent or interest as overwhelmingly in control.

Having registered these reservations may invite or even prompt the broader question as to whether retreating from the concept of moral panics simply because I find some of its contemporary uses objection is cowardly, or at least short sighted (throwing out the baby with the bath water, perhaps?). In this case, however, I feel sure that my decision to pursue another heading will not detract from other work being conducted in the moral panics vein. More to the point, my purpose here is not to make any argument about whether societal reaction was out of portion to the threat, but instead to try to understand how the issue became the subject of a broader society-wide process of problematization.

For the purposes of the present chapter therefore, I have decided to rely on the approach to securitization pioneered by the Copenhagen School[38] of security studies. The appeal of this approach lies in the fact that it circumnavigates any patina of normative judgment implicit by bracketing off questions about the validity of claims made with respect to existence of threats

[38] Securitization theory comes from the field of International Relations, but bears important parallels with sociologically grounded constructivist analyses.

and thereby avoids the conundrum of having to take a position with respect to their existence or ontological status (Buzan 1997:13). To be more precise, in this phase of the investigation the focus of analysis is on the 'processes and parties involved in 'staging as existential' threats to a referent object or population by a securitizing actor' (Buzan 1997:13).

This approach provides some immediate relief from the realist-constructivist conundrum[39] in terms of suspending questions about the validity of claims about threats, but leaves open the question of whether and how it is possible to talk about 'events' and an 'event horizon' apart from the discourses which narrate it. An analysis that proposes to bracket off the ontological plane entirely from the field of reference may create the misimpression that it is all about signification in relation to the construction of threats, and either that there are no events, or that events do not really matter. However it is important to assert positively that, on the one hand, an event or occurrence may give rise to

[39] I am aware here that a flag may be raised with respect to issues of ontological consistency in relation to approach I am articulating. To be more precise, treating narrations which describe the occurrence of events as evidence of the reality of these events while refusing to take up a position as the validity of claims made about threats (i.e. refusing to allow that these narrations denote a 'real' threat) may create the impression that there is a double standard at work or at the very least that this is a performative contradiction. However, I would contend that there is an important, if difficult, distinction to be drawn between predominantly descriptive discourses devoted to narrating the occurrence of events, and discourses which involve species of normative judgments in relation qualitative character of the conditions and/or occurrences. Moreover, while I do concede that the very question of whether an event occurred or not can be the subject of significant contestation, for the purposes of this investigation I have noted that I am not embracing a naïve or obdurate realism with respect to the processes of interpretation in regard to them. Indeed, in this context I have indicated that I am guided by Foucault's attempt to grapple with this problem by considering processes of discursive contestation involved in interpreting events, and especially, the role that expert authority may play in these processes. A deeper exploration of these issues is not undertaken here. However, for purposes of reference it may be useful to consider, as contrasting points of study on the issue, the works of Rom Harre (1986), Jurgen Habermas (1981), and Ian Hacking (2002).

certain forms of species of claims making and that, on the other hand, the fate of claims is ineradicably linked to events. Indeed, the relative success or failure of claims makers, both in having their claims treated as valid and in creating the mobilizing effect they aim at, may be influenced by emerging interpretations of events. In such contexts, the interpretation attached to a given event may negate the perceived validity of a particular set of claims, or it may have the retroactive effect of embodying the dangers previously identified by some claims makers and thus lending legitimacy to their claims.

According status to events is particularly important in the current context because, although the investigation at hand does not make any presumption about the ontological status of pedophiles or child pornographers as threats, it does nonetheless seek to understand how and why some narrations regarding 'threats' come to be seen as valid. If we want to understand what sorts of factors increase or decrease the likelihood that a given set of claims will be identified as valid and hence be seen as necessitating some sort of response, it is necessary to acknowledge both the existence of events and that these events may play a role. After all, dominant interpretations of an event sometimes serve as recurring points of reference across a variety of contexts, supporting conceptualizations of insecurity and grounding efforts at mobilization.[40] One of the impoverishing consequences associated with adopting a hard constructivist approach is the implication that it all comes down to interpretation. One of the attractions of Foucauldian nominalism in this context consists both in his willingness to

[40] Consider in this context the dominant interpretation of the events of September 11, 2001.

acknowledge the difficulties associated with identifying an event apart from the discourses that narrate its occurrence and thus his unwillingness to abandon the non-discursive realm of events and practices as a referential frame. Events cannot escape the filter of discourse, but we are not then in a position of having to contend with 'willy-nilly' narrations. Rather, when events do occur and are identified as such, we must examine why they are seen as such, and this means examining the social processes associated with their interpretation as such, as well as deliberation and debate as to their meaning. In other words, for Foucault, it is necessary to attend to the discursive processes associated with the interpretation of events as occurrences. In this context, the role of the disciplines and especially the role of expert opinion and of expert knowledge are crucial.

This observation stands out as germane for both our present and future[41] purposes. In the present context I have identified a series of salient interrogatives about how a threat becomes a danger, and how dangerousness is translated into risk. Do threats have to have been subject to some process of validation in order to be considered dangerous? Is it merely a matter of creating the perception that the threat exists for danger to be ascribed or must it be constituted as imminent? Or, alternatively, must an event occur which is effectively interpreted as an

---

[41] In terms of future purposes, in the subsequent chapters addressed to the construction of securitization solutions one of my goals will be to try to understand the processes by which actors interpret existing problematizations and adjudicate the validity of claims they embody. Claims about risks can have the effect of convincing actors that they must act upon them, and the effect of accepting the validity of these claims may even result in visible changes in subsequent behaviour. However, the persuasive effect of such claims is not a foregone conclusion. The Thomas (1929) theorem (when people 'define situations as real', they are 'real in their consequences') provides some assistance here, but we need nonetheless bear in mind the contingency of actor's successes in making their claims convincing.

embodiment of the danger? When we consult the literature on this it becomes clear that expert discourses are held to play a pivotal role. However, when we look for closer clarification in this relation we find a paucity of empirical analyses devoted to this question. In the penultimate section of this chapter I will offer a preliminary attempt to answer some of these questions by developing an argument to the effect that dangerousness is threat rendered knowable, and that risk is danger that is rendered actionable.[42]

3.3 Dimensions of Representation: 'Claims Makers and their Threats'

We can conceptualize the processes associated with representing threats to children in cyberspace in terms of the action of a variety of claims makers. However, such claims making needs to be understood against the backdrop of a broader and more generalized sense of anxiety 'parents feel in relation to the world and the safety of their children' (Jackson and Scott 1991:88). Furthermore, it needs to be emphasized that one of the most 'virulent species of anxiety over risk emerges wherever childhood comes into contact with sexuality' (Scott *et al.* 1998). As already indicated, the representations of child predators and child pornographers addressed here both bear directly upon the sexuality of the child in relation to their safety in cyberspace. In these contexts, the threats associated

[42] In short, the investigation of processes of securitization does not attempt to judge whether these claims (for example, that the presence of pedophiles in cyberspace poses a threat to children) are valid, but rather to understand the ways that constructions of the problem are interpreted and responded to in terms of problem solving. One wants to arrive at an understanding of the sorts of factors which increase or decrease the likelihood that the claims embodied in a given problematization will be identified as valid because validity is key in terms of their being seen as necessitating some sort of response.

with child predators or child pornography are rarely treated exclusively. Rather, a wide array of threats to child safety are assembled and represented. Indeed, there is instead a tendency to identify a number of 'threats' and then conflate them all into one generalized 'danger'. While it is still important to insist that the 'threats' considered here are distinct[43], we must nonetheless acknowledge that they are often lumped in with a variety of other issues. Hence, while our focus here is on risk anxiety in relation to children and, more specifically, on the sexualisation of risk and the consequences of this for children's daily lives, the analysis must of necessity stray from such specificity in order to both reflect and explore the way that these threats are lumped together with others and come to be treated as an omnibus.

Finally, before describing the findings of the analysis, is it important to emphasize that my approach to analysis was informed by grounded theory (Glaser and Strauss 1967), according to which the key categories and analytical axes employed emerge out of the data as recurring, thematic or even structuring motifs. In this context, my analysis distinguishes between descriptive and normative forms of claims making involved in processes representation. Descriptively, what we see are a variety of representations of various 'dangers' and 'insecurities' associated with cyberspace. Normatively, what we find are representations of 'responsibilities' in relation to them. Put differently, these

---

[43] To be clear about the difference, there is the danger that children might be exposed to varieties of sexually explicit content that are harmful. Such material may or may not include child pornography. And there is a second danger – associated with predators, the danger of children coming into contact with actors who are identified as sexual predators.

descriptive representations also turn out to be normatively referential, in so far as their representations of 'threats' invariably refer to and represent as 'responsible' specific agents and/or authorities as possessing the power to respond to them.[44] So we have two types of claims: discourses which make claims about the existence of a threat and are hence 'truth' claims, and discourses which are normative in character and make claims about what is 'right' (Habermas 1987).

3.4 Media Representations of the Threats to Children in Cyberspace

> A young Calgary girl was recently released from a psychiatric ward since being hospitalized for more than two months after being sexually assaulted in her home by a stranger she met on the Internet. Calgary police, armed with little more than a physical description of the attacker, are warning parents the predator might try to strike again before officers are able to identify and arrest him. 'That is my fear', Det. Lionel Busch of the Calgary police child abuse unit said Saturday. 'He could very well be, right at this moment, in a chat room doing his thing again. It's already paid off for him once.' Police say the Sept. 29 attack followed months of Internet chatting between the man and the pre-teen girl in which he carefully honed a relationship with her. He gained her trust by convincing her that he, too, was a teenager.[45]

Media representations of cyberspace can be understood as narratives that both engender fear and communicate threats. While media stories invariably feature a broad and diverse variety of claims makers (public officials, representatives from the private sector, child welfare advocates, and moral entrepreneurs from various walks), it is important to emphasize that the

---

[44] As indicated earlier, no assumptions can or ought to be made at this point about the effect or lack thereof that such representations may have on the populations they identify as responsible. One of the open questions in the risk communication literature is how and according to what processes claims about threats are adjudicated. I want to suggest that processes associated with the adjudication of claims making with respect to 'threats' 'dangers' and 'risks' ought to figure more centrally.

[45] Edmonton Journal 05/01/2003

construction of the narrative itself is the outcome of a variety of different filtering processes and editorial choices and thus, that the telling of the story is always oriented toward making it newsworthy (Ericson *et al.* 1987). Some commentators and analysts have argued that the media trade is built upon a 'discourse of fear' and is devoted to communicating at both symbolic and literal levels 'that danger and risk are central features of everyday life' (Altheide 2002). Many argue that the media are over-reliant on official spokespeople and especially formal agents of social control in relation to the construction of crime and danger. Hence, in a study that tracked media discourse over a fifteen year period and examined the use of fear in three major newspapers, Altheide showed that such usage has 'increased, that a large part of the discourse of fear includes children and the spaces they occupy and that it changed from a focus on specific events in the 1980s to a more generalized, pervasive perspective in the 1990s, peaking in about 1994' (2002). Signaling that such filtering is the norm need not oblige us to undertake a full blown review of media studies literature. It is sufficient at this juncture to point out that the dangers associated with cyberspace for children are constructed through media narratives which represent and reinforce risk perceptions and that these narratives often invoke the authority of experts to substantiate the representations they aim to render.

It would be an exaggeration to suggest that depictions of predators are pervasive throughout representations of the dangers to children in cyberspace. In fact, the possibility of predators lurking is mentioned often[46], and often in a very menacing tone as exemplified by comments from Steve Sullivan, executive

[46] Times Colonist & Toronto Star 30/04/1999

director of the Canadian Resource Centre for Victims of Crime: "They're lurking out there", Sullivan said. "It hasn't replaced malls and parks, but it has given them a new avenue. Pedophiles realize this is a really easy, anonymous way of coming into someone's house and going into a kid's bedroom to talk to them."[47] Detective Dave Johnson of Edmonton Police Services echoes this sentiment: "With the Internet, predators don't have the hassle of gaining the trust of children's family members. Instead, they can approach young people directly, either through innocuous web-based chat rooms or on chat programs that can be downloaded by kids [...] This is like a smorgasbord for predators."[48] The specific qualities of predators are seldom elaborated. In cases where they are, the descriptive characteristics provided tend to be quite vague and general. For example, in a Times Colonist story in 2000, David Toddington, an industry expert with 'a solid background in policing' asserts:

> Some people don't mind spending weeks and months grooming a child and soliciting all types of information [...] These people are very diligent. They spend tons of hours on the Internet. Some don't have lives. They spend seven or eight hours a day on this stuff.[49]

Much more attention is typically devoted to the means and methods that predators employ to gain the confidence of children and 'groom them' for a possible meeting: "Adults, often posing as children, lure kids by praising them, offering them money, gifts or jobs. They encourage them to keep their conversations secret, and then invite them to meet in person."[50]

---

[47] The Calgary Herald 02/12/2000
[48] The Edmonton Journal 22/08/2000
[49] Times Colonist 19/06/2000
[50] The Windsor Star 14/02/2000. See also The Vancouver Sun 28/04/1999.

A clear motif that does emerge in many representations of cyberspace is the general idea of 'bad online influences' or encounters with dangerous strangers. These are constructed in a number of ways. In one case, the idea is that the child may fall in with the wrong crowd online, with peers, but peers who are for one reason or another identified as wayward and capable of having a negative influence on the child. According to the testimony of one mother: "My daughter saves some of her conversations and I have now been made privy (via spying on her files) to some of them. I am totally shocked at these kids. I am shocked when adults say these things anonymously over the Internet. But 14 years old?"[51]

A second variation on this theme is the more serious and sinister.[52] The bad influences that your child is exposed to are not from a peer, but from someone who is posing as a peer, a predator.[53] Many of the narratives recount stories of a child who 'thought' s/he was talking to another child, when in fact they were talking to an adult who turned out to be a predator.[54] One particularly noteworthy instance of such an occurrence is represented in a Calgary Herald story in August 2000 in which it was reported that a Calgary police officer:

> [...] was forced to deal with an attempted Internet luring after his 16- year-old daughter made contact on the ICQ chat room with a man in the U.S. The 25-year-old man claimed he was 16 and even went as far as to send the girl fake pictures of a male teenager, alleging it was him. The pair chatted on-line for over a year and eventually the officer's daughter agreed to send the man her home address in Calgary and her phone number. The

---

[51] Toronto Star 21/12/2000
[52] Montreal Gazette 25/09/1999
[53] Times Colonist 19/06/2000; Toronto Star 23/03/1997
[54] The Vancouver Sun 28/04/1999

> man was planning on coming to Calgary to meet the girl on August 8, but the officer was able to intercept a few e-mails and stop the encounter.[55]

In so far as there have been a number of arrests in the Canadian context related to the collection and distribution of child pornography[56], and more recently, luring, narratives of such events also are often used as a spring board for a broader and more general discussion about perils in cyberspace:

> 'The nightmarish side of the 'Net includes more than 20,000 email addresses of known pedophiles and Web sites of child pornography. The briefest of searches quickly churns out a site called Nazi Pedophiles. A few mouse clicks away are web pages filled with racist diatribes, chat rooms stalked by child molesters, newsgroups poisoned by vitriolic rants [...] kids can even find 'snuff' sites where it appears victims are actually murdered online' says Mike Lawson, Net guru and software supervisor at Computer City in south Calgary. 'The Internet is particularly insidious [...] You can find virtually anything you want to find on the Internet, whether it's building a pipe bomb or sado-masochism' says Wayne Schneider, principal at James Fowler High School.[57]

There is also a persistent sense throughout these representations that a predator could be anyone, indeed that the person who is a pedophile is the one you would least expect to be one.[58] The effect of these representations is particularly heightened when the stories are related to individuals in positions of trust or authority.[59] For example a story in the Montreal Gazette relates the

---

[55] Calgary Herald 15/08/2000

[56] Coverage also frequently highlights some of the convictions for possession and distribution of child pornography on the Internet in Canada: 'In 1995, Joseph Pecchiarich, 20, of Mississauga, Ont., became the first Canadian convicted of creating and distributing child pornography by computer. He was accused of posting obscene material to an Internet bulletin board. In June 1996, a B.C. provincial court judge convicted Gerald Joseph Hurtubise and Brenda Elaine Hurtubise of Surrey, of possession of obscene written matter and child pornography. The young couple was running an adult bulletin board service'. Edmonton Journal 21/04/1999

[57] Calgary Herald 05/02/1999

[58] Ottawa Citizen 08/11/1999; Daily News: Halifax 12/09/1995; The Vancouver Sun 04/28/1999; National Post 02/18/1999

[59] Several cases in Canada have involved teachers who work directly with young people. See Toronto Star 05/10/2000 and 09/30/1998

aftershock in the community of Pointe Claire, Quebec after local high school principal David Wadsworth, an educator with a distinguished record of teaching and administration, was exposed as a collector of child pornography. In a similar case involving a high level employee at the Department of National Defense who was arrested for producing, collecting, and distributing child pornography, one of the most emphasized facts in the follow up stories was that his neighbors and colleagues thought he was such a 'nice guy' and that they never would have suspected him of such things.[60] Another high profile case reported on by the Globe and Mail in 1997 involved Nobel Prize-winning scientist Dr. Daniel Carleton Gajdusek who was arrested for child molestation after Internet activity related to child pornography was detected by the FBI.[61]

Thinking back now upon the antinomy within liberalism with respect to governing children, one of the most interesting tensions in media reports about child safety in cyberspace lies in the way they depict scenes of instigation. In some of the narratives the child is constructed as purely innocent, almost as a bystander:

> Children are easy victims for cyber-stalkers [...] Before they get to high school, kids don't have that suspicious nature. They don't think that the person on the other end of the keyboard could be dangerous. You can't see them, you can't hear them, you don't have any idea who it is.[62]

The possibility of their exposure to pornography or to a predator is described as involuntary, accidental, or attributed to the coercion of malicious child pornographers or the proactive solicitation of the child predator:

---

[60] Times Colonist and Toronto Star 30/04/1999
[61] Globe and Mail 04/05/1997
[62] Times Colonist 01/05/2000

> In one case about 18 months ago, a young teenage boy met an American man in a chat room. After they had talked several times, the man told the boy to take some money from the family and catch a bus to Vancouver so the two could meet. Then, to make sure the boy would follow his instructions, the man sent a photograph of a naked boy with a knife held to his penis and a message: 'This is what happens to kids who tell' Fortunately, the dad caught him leaving in the middle of the night [...] he was scared to death the man would hurt his family, and he was on his way to the bus.[63]

Another example of threats being used to coerce children into involuntary behavior was reported by the Vancouver Sun in April of 1999. In this case, "a teenage girl was chatting on the Internet when a message popped up instructing her to take a pornographic photo of herself and e-mail it to the man making the request".[64] The newspaper reports that the girl refused, and that the perpetrator retaliated by crashing her computer. After re-booting the computer, the girl received a second missive and this time opted to comply with the demand.[65]

While the passages above provide a good representation of the motivated predator and a good example of involuntary corruption, one scenario that received a fair amount of media attention (although it was only hypothetical) is the case of a child who is searching for 'Winnie the Pooh' online and ends up coming across a site called 'The Kama Sutra of Pooh'. The child in this case visits the site expecting to find pictures of Pooh and Christopher Robin, only to discover instead that his or her favorite stuffed animals are depicted in a variety of variously callisthenic sexual positions: "the site doesn't show naked people. But it does feature Pooh, Tigger and other stuffed animals in a variety of lovemaking positions. Such cyber-surprises aren't unusual. Many seemingly kid-

---

[63] Times Colonist 01/05/2000
[64] The Vancouver Sun 04/28/1999
[65] The Vancouver Sun 04/28/1999

friendly words and phrases, ranging from 'Minnie Mouse' to 'Pokemon', can lead a young Web surfer to images that most parents would frown upon."[66] Further support for the claim that inappropriate sites may accidentally be accessed by children appears in the March 10, 2000 issue of The Province in which Detective Noreen Waters of the Organized Crime Agency of British Columbia claims:

> In a study of 75,000 pornography websites last year [1999], more than 19,000 had been connected to sites frequently accessed by children, with linkage words as innocent as Disney, Pokemon, Nintendo or Barbie. It's called page-jacking (hacking into children's websites) and what happens is the child is suddenly confronted by these obscene images and then mousetrapped, which means they make it more and more difficult for the child to exit the site [...] I accessed a site called toddlergames and found it was 60 per cent hardcore porn.[67]

In a smaller number of cases, the curiosity of children about sexuality is acknowledged[68] and the possibility that they might actively search out sites which contain 'inappropriate content' is conceded.[69] In almost all such cases, this behavior is attributed to a lack of parenting, proper training and education about safe surfing.[70] It is, in short, a question of governing the freedom of your children.[71]

Another constant through media coverage is that the question of what actually constitutes 'inappropriate content' is vague, unspecified and nebulous.[72] In some cases reference is made to nudity, in other cases profanity. Many of the narratives stress the extent to which what is available online 'surpasses' anything

---

[66] Ottawa Citizen 08/11/1999
[67] The Province 03/10/2000
[68] The Vancouver Sun 06/08/1999
[69] Calgary Herald 05/23/1998; The Ottawa Citizen 05/22/1998
[70] Time Colonist 30/01/1995; The Ottawa Citizen 11/08/1999
[71] Calgary Herald 05/23/1998; The Ottawa Citizen 05/22/1998
[72] The Vancouver Sun 05/26/1997

comparable that might be available at the corner store or even an adult entertainment shop. Common descriptors used to describe the material include 'lurid', 'obscene', 'offensive', 'vulgar', 'seedy', and 'disgusting'.[73]

Media narrations are consistent with the broader neo-liberal logic of governance in so far as their effect is to responsibilize parents. The most definitive and profound findings of the analysis of media representations of issue of child safety in cyberspace in Canada from 1992 to 2000 is the overwhelming degree to which the issue is represented as one which is a 'problem' which parents must confront and address[74]: "the Internet can be a powerful tool, but it takes parental vigilance to keep your kids out of the cyber house of horrors that lurks online";[75] "staying involved with your child's online experiences is the best way to make sure they have healthy fun and safe adventures on the Net";[76] "young children, teens need parental road map for navigating the information highway".[77] Less than ten percent of the stories that appeared in the newspapers that were analyzed discussed the problem as one which governments ought to try to address or respond to through tighter controls, through filters or blocking or the like. In cases where other authorities (Information Service Providers or police) are mentioned, this is usually only in passing. Moreover, mention of other authorities was much more likely to appear between 1992 and 1997. And after

---

[73] Ottawa Citizen 08/11/1999. This image of the Internet was, in no small part, aided by the publication of the Rimm study at Carnegie-Mellon University, which estimated as much to 95% of Internet content consisted of pornography.
[74] Toronto Star 10/10/2000; Edmonton Journal 09/09/2000; The Province 08/16/2000; Calgary Herald 07/13/2000; The Globe and Mail 06/19/2000; Toronto Star 13/03/2000
[75] The Province 03/10/2000
[76] Toronto Star 03/13/2000
[77] National Post 03/06/2000

the decision of the Canadian Radio and Telecommunication Commission not to regulate cyberspace[78], it appears that the question of government intervention disappeared almost completely.[79] Moreover, in the few subsequent cases where articles do discuss the use of filtering or blocking software, there appeared to be contradictory positions. In one case a spokesperson from the Department of Justice Canada indicated that it was not possible to prevent such materials from circulating, but was roundly contradicted both by another government official and an ISP expert.[80]

One of the most common points of reference in many stories about the safety of children in cyberspace is polling data that indicates that other parents are worried about the safety of their children. For example, in May 2000 the Windsor Star reported on a survey conducted by the polling firm Environics for the Media Awareness Network. The poll showed that a majority of parents worried about their children's privacy being invaded online and "21% of those surveyed said their children had accidentally come across sexually explicit material."[81] These reports may have the function of reinforcing the idea that if

---

[78] The Gazette 24/05/1999. On May 17, 1999 the Canadian Radio and Telecommunications Commission released its long anticipated report in which it announced that it would not regulate new media on the Internet.

[79] An exemplary instance of the way that the responsibility for managing child security is redrawn in the neo-liberal mode is provided by Times Colonist Joe Easingwood's September 17, 2000 editorial *Web-proofing is the next step*: "it has reached the point where we have to come up with a national strategy. Not so much to regulate in the sense of censoring, but to provide parents with better information about what kinds of things kids are exposed to, and give parents, schools, and young people the ability to respond and protect themselves."

[80] National Post 28/04/1999

[81] The Windsor Star 05/02/2000

other people are worried too, 'my worries must be legitimate'.[82] Understood as narratives which communicate risk, these discourses can be understood as having parents as their 'super-addressee' (Bakhtin 1981) and as functioning to locate and constitute them in relation to their primary responsibility for 'risk management' when it comes to their kids and cyberspace. Parents are not only repeatedly identified as actors with agentive power to respond to the situation, but also are subject to a series of imperatives about how they ought and ought not to behave in relation to their children and cyberspace. Hence, several stories relate, the 'computer is not a babysitter and it should not be used as one'.[83] Children 'are often lured to inappropriate places by contacts on the Internet', warns Mayo Clinic pediatrician Dr. Daniel Broughton and although computers are a great resource for adults and children, Broughton urges parents to keep two things in mind: 'the computer is not a babysitter, and when you're online, you're in public'."[84] Another story begins with: 'When it comes to children and computers, it never hurts to remind parents that you can't leave them alone'.[85] Indeed, one story compares using the computer as a baby sitter to leaving your child standing on the corner of an intersection which is characterized by a seedy subdivision on one side – and an adult entertainment strip on the other: "If you do nothing else, monitor [...] Would you drop off your 12-year-old kid at 10 o'clock on Friday night on East Hastings? So why are you letting your kid wander the Net

---

[82] Other polling data indicates that roughly 70 to 80 per cent of parents do worry about the safety of their children online. Canadian Internet Use Survey (Statistics Canada 2005).
[83] Edmonton Journal 11/10/1998
[84] Times Colonist 07/20/1999
[85] Ottawa Citizen 03/09/1998; Edmonton Journal 27/08/1998

free?"[86] Furthermore, parents are told that rather than simply supervising their child's activities, they should take an active interest in them: "computers shouldn't be used as electronic babysitters. If you expect your child to be upfront with you, it helps to take an interest."[87]

Media narratives often represent the precautionary principle as authoritative and a good source of guidance. In this context, taking any and all measures necessary to pre-empt the possibility that your children might be exposed was asserted in a very matter-of-fact fashion.[88] For example, the use of key-stroke logging or filtering and monitoring software[89] was affirmed not simply as a good practice in cases where a parent thought that their child might be lying to them or misleading them about the nature of their online activities, but also as a general strategy of precaution in case 'something should happen'. One editorial of note which appeared in the Vancouver Province in August 1999 asked "Do you know where your kids are surfing?" The author of the column recounted her dismay at discovering that the spying systems and software she had installed on her computer had been circumvented by her son. The article subsequently provided a lengthy list of additional precautionary measures that could be pursued to interdict such circumvention. Another article from the Vancouver Sun goes much further:

---

[86] Vancouver Sun 09/24/1999
[87] Toronto Star 08/31/1999
[88] The Globe and Mail 10/24/2000
[89] The Province 03/10/2000

> Your child's supposed to be doing homework? Check the computer's list of recently accessed files to see what's there. Go to Start, Documents. A list of the most recently opened files will appear. Access a file by clicking on the one you want opened. Repeatedly press Alt and Tab at the same time to see what other programs are running and perhaps hidden behind the homework window. How to find your child's secret e-mail addresses: Try searching the child's name on e-mail search pages such as Yahoo's People Search (people.yahoo.com/). Also search for any postings they may have made to newsgroup discussions at Deja.com (www.deja.com). Does your browser silently give your e-mail address to the sites you visit? Go to www.helie.ccom/BrowserCheck to find out.[90]

Other examples which reflect and instantiate the same precautionary sentiments include: reorganizing the living room or family room, setting specific supervised surfing hours, and requiring your children to surf together (the buddy system).

In a small minority (18%) of the media narratives representing the dangers that may await children who venture into cyberspace the precautionary principle was not represented as viable; the idea that children 'may' come across 'inappropriate content' was instead asserted as an inevitability.[91] As one story puts it, 'the question is how you will deal with it'.[92] The stories in such cases typically segue to the question of harm reduction strategies, the implication being that the child has been contaminated, and that the question is how to 'treat' them.[93]

---

[90] The Vancouver Sun 09/24/1999
[91] National Post 05/03/1999
[92] Calgary Herald 23/08/2003; Kingston Whig Standard 09/11/2000
[93] While many more themes emerged out of the analysis of media coverage of child safety in cyberspace – I have reserved further discussion of the section devoted to questions of emplacement in order to treat it there in a more direct relation to the constitution of parents as risk managers.

3.5 Marketing Fear - Retailing Security

Just as parents are the principal target in most media coverage regarding issues of safe surfing and responsibilization, the target demographic in the case of marketing is parents, not the children. For those engaged in the business of selling security, creating market demand is a matter of materializing danger, making it palpable and immediate so that the threat to children is not only clear but appears imminent. It would be simplistic to imagine, of course, that these marketing strategies in and of themselves create a climate of fear. Indeed, as mentioned previously, it is far more accurate to say that the climate is already in place, and that the strategies used by marketers merely play upon and function to intensify anxieties around the safety of children. When we look at the product advertising and packaging we see there are several strategies at work in this regard that are consistent both with the logic of the market and with the larger individualizing logic of risk in neo-liberal societies.

There is a moral subtext common to all strategies aimed at convincing parents of the need to purchase filtering or blocking software. This rationale is also present in other solutions such as keyboard logging or chat monitoring equipment. Simply stated, having been informed of the grand manifold of dangers and dangerous individuals, securing the safety of children in cyberspace is presented as the moral responsibility of parents.[94] Such moralization as a general strategy zeros in on a parent's sense of right and wrong, of duty and obligation, and perhaps most importantly of fear.[95] One of the foremost or

---

[94] Also see The Province 10/03/2000
[95] Also see the Gazette 22/06/2000

paramount obligations of parents is to protect their children from harm. And one of the most terrifying forms of harm is a violation of the child's sexual sanctity. For parents, this may amount to exposure to sloganeering that aims to incite one to vigilance with haunting interrogatives like 'do you know what you child is doing in cyberspace' followed by menacing facts such as: '1 out of 5 children have met someone in the real world whom they first met online'. Many marketing strategies used by the manufacturers of these products rely on such statistics. The effect of these strategies may be that the problem is redefined: it is not simply that there are bad guys out 'there', it is also that you, as a parent, do not know what they may be doing. A repeated message throughout these narratives is that danger is immediate:

> In words and in pictures, even hard-core pornography involving kids and animals is available on the Internet if you know where to look and it's all as close as the children's section at the public library.[96]

Further persuasive power is provided by first hand testimony, alliances with respectable hardware and software providers and a litany of endorsements. Product packaging typically features both testimonies from experts in the industry and from average parents providing compelling anecdotes and cautionary tales:

> I had become increasingly worried about the time my daughter was spending on the computer in her bedroom. I didn't know enough about computers to find out what she may have been hiding, but I found your product, installed it and was shocked to learn what was she was doing and who she was talking with online. Because your software is easy for someone like me to use, I was able to know when my daughter needed some parental intervention. Thank you for making something like this for a busy, single mother like myself.[97]

---

[96] See the Daily News – Halifax 12/11/1995

[97] Net Nanny testimonial http://www.netnanny.com/p/page?sb=detailed.

Perhaps the most important action in consolidating the claim that children surfing unprotected in cyberspace are in danger consists in alliance building. Net Nanny, one of the most successful companies at the level of market share, has built a broad network of alliances with all of the major players in terms of information technology, hardware providers, and software developers. Building alliances allows for the formation of networks to legitimate their claims and also, in a kind of reverse rationale, indicates that the threat must be real since there is such an extraordinary effort underway to address it.

3.6 The Panoply of Experts

Expert testimony plays a critical role in problematization. Through pronouncements made in the public sphere or in the media, experts are seen as more believable about levels of threat and/or dangerousness and they also play a critical role at the level of securitization by proffering advice and judgments about what should be done in response. It is important to acknowledge, however, that although experts play a central role in risk discourse, they are not the only experts. Beck reinforces this idea by saying that 'in matters of hazards, no one is an expert - particularly not the experts' (1992:106). Others argue that the lines between scientific experts and non-experts have become increasingly blurred in a society where risk logics are prevalent (Johnston and Shearing 2003). Beck emphasizes that a wide range of actors may make competing claims about risk and end up vying for public support. In this context, personal victimization in

cyberspace can be seen to constitute one as an authority. Other claims makers who may come to be seen as legitimate authorities include security specialists, long-standing contributors to particular communities and lay people by the very virtue of their lay status. To say that membership in the expert opinion category is wide ranging is also to acknowledge the extent to which expert opinions reflect radically different conclusions. Some experts are all too eager to validate claims aimed at problematizing the presence of children in cyberspace, while others contest these claims as specious or exaggerated.

Amongst the variety of experts invariably paraded out to communicate risk, police serve as a primary resource in media reporting, as they are in media reporting on crime more generally (Doyle 2003). Indeed, more than forty percent of the articles examined featured solemn avowals by police not only about the current extent of the danger, but also included claims that the threat is growing. In some cases, these avowals are accompanied by descriptions of new initiatives being pursued by the police and discussions of the intended effects and target populations. Sometimes the police play the role of the morally affronted: says Peter Gulotta of the Baltimore FBI task force, "Of all the cases I've worked, Internet predators are the most reprehensible I've ever seen."[98] In such cases, there is no reason to call into question their categorization as experts, though their value neutrality certainly should be questioned:

> 'I find it absolutely disgusting and abhorrent that anyone can get any kind of sexual gratification out of children who are that young,' Det. Staff Sgt. Bob Matthews of the Ontario Provincial Police told a news conference yesterday.[99]

---

[98] Toronto Star 08/05/2000
[99] Kingston Whig Standard 11/12/1996

Garland (2001) has argued with compelling evidence that scientific expertise has turned the management of risk into a business. Computer security, at the most general level, is certainly an industry devoted to risk management. The development of epistemic bodies of systems expertise is therefore central to subsequent processes whereby individuals are instructed to modify their conduct according to risk. Computer security experts also play a key role in both substantiating and instantiating discourses associated with threats to children in cyberspace. Their role extends beyond descriptive claims making, in so far as they are also instrumental in establishing behavioral norms about how others should use and relate to technology. Hence, we find that systems security experts frequently make reference to what could be constructed as the 'prudent' user (O'Malley 2001), a person who practices proper computer hygiene. For example, by changing passwords regularly, using firewall and anti-virus applications, and obeying the prohibitions against opening emails from unknown sources. The popular conception that experts do not assume moral positions is especially suspect in the context of systems administrators or experts who are available for help at Bell Sympatico or Rogers At Home; one is admonished never to download software from a source that is unknown or unreliable, never to open an attachment to an email that is from a person you do not know, and not to click on an email from someone you do not know. The accumulated knowledge of these experts is directly linked to risk discourses which address unsafe behavior in cyberspace and includes a variety of imperatives. As we will see shortly, these experts do not simply collect information; they subject it to sundry

processes of interpretation and translation which reflect a conception of security consistent with their interests (Kinsmen 2002).

Victims may also seek and find representation under the rubric of expert witnesses or give expert testimony. Indeed, some of the most powerful voices emergent in relation to the threat of child predators and pedophiles comes from communities of expert victims. In fact, these need not be victims of online luring, but may simply have survived child sexual abuse. In two cases in media reports, the survivor status of these victims features formidably in terms of constituting their authority as well as showcasing the solutions that they think are necessary to deal with the problem. Moreover, a good number of sites on the Internet devoted to opposing or combating child pornography are run by victims. The personal experience of victimization in these cases provides an authoritative foundation from which to render judgments about how 'bad it is out there'.

In one of the most interesting instances of arguments from authority, cyber-activists and vigilantes have sometimes been constituted as experts. The group 'Perverted Justice' is perhaps the most prominent example of this phenomenon. I shall have much more to say about this group in the chapter addressed to intervention, but for the time being it is worthwhile to note that they have played a very high profile role in the recent series 'To Catch a Predator' put together with NBC's program 'Dateline'.[100] It is difficult to underestimate the

[100] The first episode of 'To Catch a Predator' (which actually began as a single installment show and was not intended to be a series) aired in 2004. According to NBC, the popularity of the program and the issues it uncovered prompted it to develop the program into a series format. As a matter of fact, the show has prompted other stations to do copycat shows, including CTV in Canada. The show is organized in the following way: in the months prior to shooting each episode of the program, NBC makes

sensation and stir this program caused across law enforcement communities in the United States. What is noteworthy is that the expertise of the individuals who volunteer at this organization has been reinforced by officialdom. A number of police departments have engaged the group to provide training to their members in the monitoring of chat rooms and in the capture of sexual predators. These individuals are routinely contacted by media in matters of child abduction or luring and can be counted upon to give solemn avowals about the seriousness of the problem and the degree to which conventional law enforcement is not able to address it.

3.7 From a 'Threat' to a 'Danger' to a 'Risk'

Having reviewed some of the kinds of claims making involved in representing the threats that children may encounter in cyberspace, it remains to offer an analysis of the distinction I want to draw between threats and dangers and to locate this argument in terms of a larger theoretical framework. Firstly, it should be indicated that I openly acknowledge that, in popular discourse, the terms 'threat', 'danger', 'risk', 'hazard', and the like are used interchangeably and

---

arrangements with Perverted Justice volunteers such they later agree to focus their efforts on developing relationships with men (a woman has not been featured as of yet) in a particular geographical area. They do so by frequenting geographically specific chat rooms and doing the requisite decoy work: posing as underage boys or girls. The aim is to develop and cultivate a sufficient number of promising contacts with men that appear to be interested in meeting. NBC then rents a house (termed the 'undercover house') which it fits extensively with cameras and provides the address of this house to Perverted Justice decoys who then provide it to the men who are targeting them for the purposes of setting up an appointment to meet. When the online contact arrives at the undercover house he is met by a child model whose purpose is to draw the man into the house. Once inside the house the man is then confronted by Chris Hansen, who is the host of the show. What follows afterward is usually a process of interrogation in which Mr. Hansen challenges the men to explain what they are doing at the house.

that my intention in staging this intervention is not to induce the general or even academic public to exercise more care in its use of these terms. However, I do think it is necessary to have recourse to a vocabulary or lexicon that affords more precision in order to better understand the representations contained in claims.

It will be recalled that it is my argument is that claims about threats have a highly contingent status. Indeed, that claims about threats are the weakest forms of claims making, as almost anything can be conceived of as potentially threatening. However, in the event that an incident occurs that seems to confirm, or is interpreted as confirmation of the validity of a threat claim, then threats are immediately reinterpreted and reassigned the status of dangers. In other words, when events are interpreted as instances of the realization of a specific threat, the threat is no longer simply a threat at all, it is a danger. Dangers can be distinguished from threats in the sense that the former are embodied and hence have an empirical basis. This empirical basis is critical to the next phase - in which dangers are translated into risks. Translating dangers into risks means specifying their conditions of possibility. Once these conditions of possibility have been specified, then dangers and dangerousness are in a sense rendered actionable.

In this section I discuss the role of expert knowledge in the processes of translating dangers into risks. My supposition in this context is that, as a result of their shift in status from hypothetical to actual, from mere threats to embodied dangers, Internet predators and child pornographers become available as subjects susceptible to, and suitable for, scientific study. And further, that the

knowledge constituted under the auspices of such investigations is critical in rendering the dangers these population pose as intelligible and the risks they represent as manageable. The preconditions for the possibility of such studies are, of course, an already existing reservoir of normative knowledge about healthy sexuality and the concomitant application of normalizing judgments to all of the populations in question:[101] children, child predators and child pornographers. These processes through which dangers are translated into risks are critical because they make 'security' a viable and actionable objective in so far as they nuance, qualify and quantify the character and nature of the danger for children and the dangerousness of child predators and child pornographers, and thereby render it amenable to risk logics[102] and susceptible to forms of address aimed at management through securitization strategies (Dean 2004:117).

While my argument with respect to the character of risk relies on a Foucauldian framework for some direction, I am here attempting to press beyond it. In the Foucauldian frame, risk as a logic is associated with neo-liberal modes

---

[101] In advancing this argument, I am relying on Foucault's analyses of the ways in which disciplinary power operates and, in particular, of the logics associated with the constitution of the dangerous individual.

[102] Several approaches to risk are extant in the literature. The first, associated with Beck, postulates a stage of development wherein society is fundamentally structured around and oriented toward a series of risks that have developed as a result of increasingly complexity and technological development. The second approach, following Douglas and Wildovsky, postulates that risk has taken hold culturally and become a dominant way of interpreting the world (2004). The third approach, which comes from Foucault and has been developed by Ewald, Hacking and Dean, amongst others, posits that risk is a tactic or technique that is coincident with neo-liberal forms of governmentality. According to this latter approach, risk logics are polyvalent and susceptible to deployment under a variety of strategic objectives.

of governance.[103] On this account, it is crucial to remember that risk is associated with danger, but the two are not equivalent. Risk is always imagined in relation to specific contexts and historical moments. Moreover, risk discourses elevate safety and security to the level of primary concerns through processes of specification. While the construction of danger and dangerousness is the ongoing outcome of a variety of actors (including the mass media, government, legal professionals and a plethora of other actors and agents), I want to argue that the epistemic status of risk is distinct from that of danger. Risks are dangers that have been subject to processes of epistemization and thus claims about risk are based upon references that relate to probability and calculability.

Given this set of stipulations with respect to risk, it remains to acknowledge the role that the processes associated with the constitution of social scientific knowledge about cyber-predators and child pornographers increasingly plays in relation to cyberspace. Of course, it hardly needs to be pointed out that the classifications of cyber-pedophiles and cyber-child pornographers are derivative of the more basic categories of 'child predators' and of 'child pornographers' that were prominent in criminological and psychological literature long before the advent of cyberspace. This is not to say, however, that a distinct body of empirical knowledge has not developed in relation to these activities when they are committed in cyberspace. Indeed, both areas are burgeoning with new research and the knowledge they produce is in high demand by police forces and other organizations around the world.

---

[103] This position has been identified as resolutely nominalist with respect to the question of whether risks actually exist – which is broadly consistent with my overall approach.

3.8 Summation

The aim of the two previous chapters was to situate the representation of the threats and dangers posed to children by the Internet against a broader background context characterized by complex political and economic commitments. This work showed that neo-liberal rationalities of rule played a role in both conditioning the way that these dangers and threats were represented and also in influencing the way that they subsequently came to be interpreted in terms of risk. I argued that the result of such representations and interpretations was a gradual and progressive condensation into what I have dubbed the securing-child-safety-in-cyberspace problematic. This work was important not only because it showed that a diversity of claims makers were involved in representing a wide variety of dangers associated with cyberspace but more importantly because it established that one of the effects associated with such representation was to render them governable at the level of risk through strategies of securitization.[104]

For the remainder of this work, the focus will now shift away from an analysis of the formulation of the child-safety-in-cyberspace-problematic and toward an analysis of processes associated with the development of socio-technical solutions in response to this problematic. The questions investigated from here on in are how the risks associated with the insecurity of children came

---

[104] Recall Dean's claim: 'risk is a way of representing events so that they might be made governable in particular ways' (1999:131). It should also be recalled that securitization is only one of three available processes of governmentalization associated with the social construction of the Internet.

to be operationalized as actionable and how they came to be acted upon through the selection of specific strategies and tactics. Making this shift does not mean that we can now dispense with any and all questions of representation and interpretation. Rather, it must be acknowledged that we are still dealing with issues of representation and matters of interpretation in the particular problem solving contexts that will be examined. Indeed, decision-making in these contexts may be informed by differing understandings and conceptions of the nature of the risks at issue, and of the parties responsible in terms of mounting a response.

Chapter Four:

Problem Solving and the Construction of Socio-Technical Solutions

4.0 Introduction

This chapter is devoted to developing a theoretical framework sufficient to ground an analysis of the processes associated with the development of socio-technical strategies which are aimed at addressing the securing-the-safety-of-children-in-cyberspace problematic In order to characterize these processes, we must have recourse to a both macro-logical approach (which can address why the security and safety of specific populations might become an ongoing concern and how systems forces and structural factors may influence trajectories of development) and a micro-logical one (which can address how cognitive understandings may inform the behavior of actors). We must further view them in multiple contexts from the micro-theoretical to larger sets of structuring logics associated with neo-liberal modes of governance and risk rationalities. My approach to the development of such a framework is threefold.

First, I briefly survey the extant macro-theoretical and micro-theoretical traditions associated with explaining processes of technological development, looking particularly at the factors and forces they single out as important, and at how these do or do not apply in the case of the Internet.

Second, in so far as the exposition reveals a propensity to conceptualize contexts of design as distinct from, and prior to, contexts of operation and/or emplacement, I argue that the case of cyberspace is unique in so far as we

appear to be dealing with a techno-social domain that is design (or construction) all the way down. Following this line of argument I contend that traditional literatures predicated upon a conceptual commitment to thinking and keeping science, technology and society separate[105] are inadequate to the task at hand. To be more specific, such approaches invariably resort to a series of 'boundary maintenance strategies' (Brown 2006) in order to preserve the separation that they presuppose.

Third, having illustrated the shortcomings associated with these traditions, I turn my attention to more recent work drawn from the social studies of science and technology tradition and from social construction of technology studies. Here we find a toolbox of concepts that are of assistance in conceptualizing the processes associated with problem solving and the social construction of security solutions across contexts. My aim is to recoup the critical insights contained in these more recent theoretical developments in order to integrate them into a tri-ocular framework for understanding the processes associated with problem solving in terms of a strategy of securitization. I suggest that a comprehensive conception of securitization must begin by acknowledging its rise to the status of a general imperative, the processes whereby security is problematized in relation to particular populations, and finally, how concerns about child security were

[105] It is perfectly legitimate to query whether a specific technology emerged in response to social demand (i.e. whether necessity was the mother of invention) – or alternatively whether in the process of its emergence a specific technology created a demand for itself (i.e. whether invention was the mother of necessity). However, these abstractions result in a form of essentialism that impoverishes our understanding of ourselves and our relationship to technology. Indeed, as Feenberg notes, this idea 'turns on a sharp distinction between the technical and society, and this distinction has broken down' (1999).

implicated in the processes of interpretation, contestation and stabilization processes associated with the social construction of securitization tactics.

A variety of historical and theoretical approaches have been brought to bear to explain trajectories of technological development. Rather than organize my overview along disciplinary lines, however, I have here elected to adopt a broad distinction between internalist approaches to explaining the logics which shape trajectories of technological development and contextualist approaches to the explanation of the logic which steers technological development. The logics of analysis and explanation that underlie traditional approaches to explaining technological development typically rely upon some commitment to keeping science, technology, and society separate. Although the supposition of such a separation has since been called into question, the legacy of these literatures cannot be overlooked in so far as they have pushed cause or effect questions to the foreground.

4.1 Endogenous Explanations of Technological Development

For a long time, studies of history of the development of technology were dominated by what has become known as the internalist approach, according to which trajectories of technological innovation and development are linked to endogenous factors like the logic of scientific discovery (Hughes 1986). I want to distinguish between two varieties of internalism. Weak internalism assumes that the values involved in making decisions about directions of programs of scientific research are relatively autonomous, but allows that whether and in what ways such knowledge actually ends up being incorporated in future technological

design and development is neither given nor can be assumed. Strong internalists, on the other hand, are confident that the knowledge yielded in processes of scientific discovery finds its way into the subsequent design and development of technological artifacts and or systems. According to this latter line of explanation the invention of artifacts or systems follows an almost inevitable chronology and linear progression in which the logic of scientific discovery is determinative: 'As less complex and efficient machines, devices and processes gave way to those that were more so, and as limited applications of the technical devices were superseded by far more numerous ones, the authors of these histories began to believe that technology displayed an inherent logic' (Hughes 1986).

Some Marxist analysts have advanced a strong internalist position in the explanation of technological development. In opposition to the contention that 'scientific knowledge must be treated as an outcome of specifiable social processes', they argue instead for the relative autonomy of science (Mulkay 1972:18). For Marcuse, the trajectories of technological development that follow in the wake of scientific progress are politically biased in their intrinsic form, not simply by the specific demands capitalism places on them in the application (Feenberg 1994:26). Some internalist accounts of the logic to scientific discovery go so far as to accord such logics an autonomous role in determining in the course of technological design and development. Hence, Castells introduces a distinction between the capitalist mode of production and the informational mode of development in dealing with the impact of the new information technologies.

While the former denotes the broader system of production ruled by the market imperatives of profitability, the latter designates the socio-technical structure which provides the means to generate a given level of production. Castells argues that *social arrangements* and *technical requisites* are inter-related but relatively autonomous. Hence, taken historically, societies demonstrate transitions from predominant modes of development. Information processing is hence a new technological paradigm and as a socio-technical mode of development it is the 'fundamental activity conditioning the effectiveness and productivity of all processes of production, distribution, consumption and management' (Castells 1994).

Internalist histories of technology have fallen into disfavour for two reasons. First, they either outright neglect or gloss the role that broader sets of values play – both in terms of determining direction of research and investigation and in processes of design and development. In the former case, the account of the logic of scientific discovery is simply specious. To begin with, in scientific settings researchers select, out of a variety of possible directions, which one they wish to pursue in terms of further experimentation – but they do not do so in isolation. Their choices are based on a calculus that includes, among other things, the interests and beliefs of the researcher, monies available, the perceived value of the various lines of research, the body of existing scientific knowledge, and the costs and potential payoffs. Over hundreds of years, vast pools of scientific knowledge have accumulated in this way and these reflect the values underlying such processes of calculation. In other words, much of the pool

of existing scientific knowledge more or less reflects the kind of knowledge that some groups of human beings have deemed valuable and worthy of acquisition.

In terms of design and development, decisions must be made based on judgments and in order to make such judgments decisions must also make reference to some constellation of values. A plethora of recent research suggests that there is no logic of necessity that orders and informs the processes underlying a given technology's development. Rather, design and development contexts are characterized by a multiplicity of contingencies and the processes of addressing them involves human choices, values and beliefs (Latour and Woolgar 1974). Engineers and designers may draw upon these vast pools of scientific knowledge when they try to invent an object that will harness the natural processes discovered through science to perform some particular function, or meet some human need. Of course, in this case, the choice of means available to the engineers is limited by the sum-total of available scientific knowledge. Hence, they are constrained to some extent an antecedent set of choices made in the area of research. Furthermore, the engineer in turn engages in a calculus of his/her own where he or she makes decisions about design, function, form, economy and the like based on his/her own values. Yet another process of calculus is involved at the level of production where quality is balanced off against cost.

Finally, it is noteworthy that internalist accounts give little consideration to contexts of emplacement. Choices and values are involved here too. Not only can people say yes or no to new technologies, but the uses that they chose to

put them to are under-determined by the intended uses designed into the objects. There is no guarantee that the technology will be used to do what it was intended to be used, which is not to say that the spectrum of possibilities for use are unlimited [106], but only that interpretive flexibility is the rule at this level too. Between the 'intended use' as reflected in the objects design and the 'actual use' which varies according to contexts of emplacement, there are some, but not unlimited, degrees of freedom.[107] To complicate matters further, there is no guarantee that a particular tool, technique or technological object will do only what it is supposed to do.[108] As Hughes (1986) argues:

> This kind of history can be written if the historian does not attempt to explain technological and scientific change by following causal connections wherever they may lead – but tries only to describe change within categories rigidly disciplinary containers.

4.2 Exogenous Explanations of Technological Development

The dominance of internalist approaches to the explanation of trajectories of technological development initially elicited resistance and ultimately resulted in the development of an opposing camp which has become known as the contextualist approach. In this approach both 'the notion that science is the context of technology' and the idea that 'technology is merely applied science' is rejected. Innovation studies have largely been dominated by the field of

---

[106] The activity of computer hacking is likely paradigmatic here.

[107] I have in mind the by now well know case of Minitel - a communications bulletin board established by the French government which became, by sheer fiat of Minitel users - a conferencing centre for prostitution, drug dealing and other unlawful activities (Castells 1996). A second, more dramatic example is provided by the case of Canada's sale of Candu reactors to India. The reactors were used to produce nuclear energy, but also were used to produce cores used in India's construction of the atomic bomb.

[108] Cars for example, are intended to provide rapid locomotion - but they were not intended to produce gases which would deplete the ozone layer.

management and economics and have overwhelmingly tended to address macro-economic environmental factors in accounting for innovation (Layton 1977:189). In this context, internal dynamics which may influence the development of technology (like limitations of scientific knowledge) are not treated directly. This has lead Layton to lament that 'technology is often assumed to be a 'black box' whose content and behaviour may be assumed to be known by everyone' (Layton 1977:189). These studies may contribute to our understanding of the conditions for economic success, but to the extent that they do not inquire into the content of technology they cannot be used as the basis for a social constructivist view of technology' (Bijker 2002).

A second tradition that bears continuities with contextualism and is associated with Marxism is the political economy approach. This approach holds a very different view of the logic of scientific discovery and of the relationship between science, technology and ideology. This second tradition takes its lead from Marx's conception of the relationship between individuals, activities and conditions and the world of essences. In this context, the production of scientific knowledge cannot be conceived as an abstract process but rather involves the material manipulation of natural phenomena and contributes to the reproduction of specific sets of class relations. Hence, Marx sees the growth of scientific knowledge as concomitant with the emergence of capitalist society (Mulkay 1972:5). And, as scientific knowledge is employed to increase the efficiency of production, the resulting increase in the pool of resources allows science to expand. Hence, not only does science develop in a reciprocal relationship with

the capitalist economy, but capitalism directs the development of the natural sciences in a drive toward technological innovation (Mulkay 1972:6). This conception of the relationship between science and technological development is key for Marx.

Political economy approaches emphasize the degree to which the logics of scientific discovery and technological development are codetermined by larger social forces. Grounded in a systematic analysis of capitalism, political economy approaches argue that capitalist forces are at the root of both the historical evolution of, and recent trends towards, information development. Focusing on the link between the new information technologies and the vicissitudes of advanced capitalism, they argue that proprietary structure largely determines content, patterns of ownership, sources of advertising revenue, and that market considerations condition both technological form and content. In this context, Dickson sees the development of information technology in terms of a dynamic interplay between the corporate sector and the military-industrial complex (1984:67). Kellner, on the other hand, posits a gradual convergence of capitalism and the information infrastructure in terms of a transition to techno capitalism: 'a period where new technologies, electronics and computerization displace machines and mechanization, while information and knowledge come to play an increasingly important role in the production process, the organization of society and everyday life' (Kellner 1989:171).

Schiller offers an interactive model that is more nuanced: information infrastructure not only develops in response to capitalist imperatives but, at the

same time, informational developments support the capitalist system. The rise of information technologies is, indeed, indissociable from the history of capitalist development, but information must be understood as both the essential foundation of that historical development and its ongoing condition of possibility. One the one hand, class based power structures are at the epicenter of the information infrastructure, and these interests determine not only the development of technologies, but also the spectrum of opportunities available for their access and application, and the interests underlying proposed changes and innovations. This is true not only because the profit motive rules unchallenged as the fundamental determinant of both the rate and direction of the development of information and communications innovations, but also because market criteria determine the quality and quantity of the information itself and thus result in a general commoditization of information. More specifically, the logic of corporate capitalism ensures that communication developments continue to serve private, as opposed to public, ends. Although the information revolution is occurring on a global scale, it is both marked by existing inequalities and may also aggravate them: the information gap may increase.

In the Canadian context, a variety of analysts and scholars of the Internet have taken their lead from a political economy approach. These approaches emphasize the role played by economic forces and motivations in the development of the Internet. Several analyses grounded in the political economy approach have focused on the role played by the state in determining the Internet's direction of development. Gutstein (1999) for example, develops a full

blown analysis of the approach to Internet development in Canada, arguing that this process has been one characterized by enclosing the electronic commons. 'Connecting Canadians', the Federal government's comprehensive strategy to make Canadians the most connected people in the world, is a program that aims to domesticate cyberspace and enroll Canadian communities, businesses, and individuals in a project of self-transformation. According to the political economy approach, discourses devoted to security are a matter of protecting property.

Many scholars have suggested that a stage model offers the most felicitous approach to understanding the process underlying the development of the Internet. An assortment of overlapping stages have been proposed that would describe its' trajectory of development. The first stage is generally identified as a characterized by government ownership and a plurality of interests operating on the Internet without any overall co–ordination of aims at the level of modification of instrumentation. In the second stage, usually described as privatization, the Canadian government sold all of its network holdings to the private sector and legal and regulatory structures were established to secure private ownership and establish 'pay-per-user' system. In the third stage, commercialization, the Internet is identified as a great place to do business and the dot.com revolution ensues. The fourth stage, corporatization, is characterized by concentration of ownership.[109] Some disconsolate theorists prophesied a fifth stage which would be characterized by monopolization and would have the consequence of stripping the Internet of the liberating benefits associated with

[109] This is a rough and ready reading of such stages partly because I am dubious about the value of thinking about periods in the development of the Internet in Canada as solely determined by ownership issues.

the extended communicative capacities enabled by the Internet and creating a system of communication that is under complete control (Kroker 1994).

4.3 Interactive, Reciprocal and Recursive Relations

Dissatisfaction with division between internalist and contextualist approaches has led many to propose that the relationship between science and society, between technology and society, and between science and technology ought to be understood in much more complex terms and as much more fluid and interactive than previous conceptions had allowed. In the context of science and society studies, the attention to other 'so called contextual factors, social, political, economic' paved the way for this 'interactive' emphasis. In this section I examine approaches to the explanation of trajectories of technological development predicated on Interactionist approaches. These are of two kinds – those that opt for a macro-level explanative orientation – and those that operate at the micro level. Most of these approaches precede from the assumption that technology and society – or subjects and objects - must be thought of relationally, but the basic binary between technology and society is not, in and of itself, ever challenged. In the exceptional cases of Heidegger (1997) and Habermas (1968), however, we see that some sort of dissolution of the distinction seems to be in the works – either by having technology absorb society through a process of ontological reconversion (as in Heidegger) – or by a fusion of science and technology that threatens to colonize society.

Giddens (1971) offers a macro logical critique of the political economy model and an attempt to develop a more specific analysis of trajectories of technological development by bringing in the exigencies associated with bureaucratization and the modern nation state. Informed by Foucault's analysis of carceral networks and Adorno's account of the administered society, Giddens embraces the idea of interdependence and a conception of codetermination: the evolution of highly complex modern societies is indissociable from the rise of specific formations of informational structures, and the development of expert systems which systematically aggregate information for the purposes of strategic planning. Routine surveillance is a precondition for modern nation state formation in so far as, at the inchoate stages of their social organization, states define themselves geographically in order to define who belongs and does not belong, and exercise political power accordingly. Since the survival of nation states depends of their ability to plan for the administration of resources and protect and exercise authoritative resources, Giddens argues, they require effective systems of surveillance. The institution and ongoing management of this information gathering and storage apparatus contributes to the formation of national identities, which allow states to exercise sovereignty at political and socio-economic levels. Second, in so far as nation states are typically born under conditions of war, the claim to sovereignty requires that national governments uphold the integrity of their borders. Preparedness for war is a requisite of all nation states.

In Habermas we find a broad ranging critique of technology as a basis for social organization. Drawing from Marcuse, Habermas argues that the general dissemination of science and technology has contributed to the development of a widespread positivism that, when combined with broader processes of rationalization, culminates in an orientation toward purposive-rational action that ultimately undermines the emancipatory potentials of communicative action and thereby result in a *colonization of the lifeworld* (Habermas, 1968: 81). Habermas locates the link between 'rationalization and the institutionalization of scientific and technical development' (1968:81) at the level of societal steering structures and argues that these have become increasingly dependent on empirically augmented reason. Technological rationality thus becomes insinuated in purposive rationality more generally, as science places technique at the disposal of steering systems (money, power) for the realization of specific goals (McCarthy 1978: 8). This conjunction leads to the development of a specifically technocratic form of consciousness which Habermas identifies as 'less ideological than all previous ideologies, because it makes a fetish of science' (1968: 111). This consciousness insulates the hegemony of empowered classes in so far as it is renders structures of domination less vulnerable to reflection, and the positivist structure underlying it maintains the projected force of truth. The result is a society-wide orientation toward the exercise of control that culminates in the fact that rationalization becomes 'a specific form of unacknowledged political domination' (1968: 82).

For Habermas, technology not only contributes to the ascendancy of purposive-rational action. Combined with the mantle of positivism, it inhibits the development of norms that are consensually arrived at through communicative action. Habermas calls the specific conjunction of technology and science that leads to this hegemonic formation in capitalism the 'scientization of technology' (1968: 104). More specifically, Habermas claims that the application of science to technology leads to a rationality of domination to the extent that purposive-rational action is increasingly governed by 'technical rules based on empirical knowledge' (1968:91), and rational choice becomes increasingly based exclusively on analytical knowledge. What is key about the scientization of technology, according to Habermas, however, is that it eventually results in a condition in which technological progress comes to be seen as an independent variable upon which economic growth depends. According to this ideology 'the development of the social system seems to be determined by the logic of scientific-technical progress' (Habermas, 1968:105). As this scientific-technical logic develops the force of empirical authority, it legitimates the decline of democratic decision-making about practical problems by making them appear as though they are subject to technological solution, thereby fertilizing the ground for a full fledged technocracy (1968: 105). Scientific-technology thus 'becomes a background ideology that penetrates into the consciousness of the depoliticized mass of the population, where it [...] take[s] on legitimizing power' (1968:105).

4.4 Micrological Approaches to Understanding Interaction

In the phenomenological approach we find the presupposition that technology and humans are so closely intertwined that to examine one it is necessary to examine the other. The factors which contribute to the design decisions are so deeply embedded in the prevailing social and cultural milieu that does not make much sense to talk about them as abstracts. Dispensing with the conception of technology as applied science, it focuses on the fulcrum of techniques that constitute human technological praxis (Idhe 1986:84). This shift displaces the linear interpretation of technological development with one that is reflexive. From this perspective, Idhe argues, shamanic magic can be seen as a 'technics of religion' and united with Western practices at the hermeneutic level (1986:83). However, technics for the former is an analogue of language rather than 'an extension of the body' (1986:83). Indeed, in the latter, technology is narrowly understood 'as a physical force limited to an implicit model of the body and its extensions', thus rendering invisible the hermeneutic dimension (1986:86). Taking up a median position between these two traditions, phenomenology focuses on 'the materiality of technics in all human praxis' (1986:84). A precondition for this possibility, however, is a disclosure of the way that the hermeneutic dimension of technology is culturally embedded.

On the basis of this analysis, Idhe asserts, amplification power can be understood as an invariant dimension of technology. It is this that allowed humans to prevail over species with greater natural strength and to prevail over nature itself. Just as the text 'embodies' and transmits religion, so

instrumentation 'embodies' contemporary science' (1986:86). It is not enough however, to insist that contemporary science could not exist without instrumentation even though its primary fields at the micro-macro levels are made present through technologies of instrumentation. Indeed, a radical shift is required to overcome the view that technology is applied science and apprehend the role of technics in human activity (1986:85).

Finally, for Heidegger 'the environment we live in becomes an artifact of the omnivorous future of the technological system' (Heim 1993:66). The preponderance of technological systems culminates in an all enframing *Gestalt* that terrorizes thought by virtue of lack of specificity. Heidegger's key claim is that as the essence of technology comes to pervade all of human existence, it creates inestimable dangers, transforming human beings and altering (almost irreparably), human actions and aspirations. The problem for Heidegger is not that 'machines run amok or that we come to understand ourselves in comparison with machines' (Dreyfus 1972), but rather that technology becomes a mode of human existence. McLuhan sees technology as transforming the human environment by altering its content to such an extent that the environment itself becomes the artifact. Heidegger's essential claim in this context is that technology is not simply a collection of tools neutrally used by humans, or even that it is a way of seeing, but rather that as enframing it becomes a hermeneutic background. This is the thesis of ontological reconversion that is at the heart of his analysis. More specifically, through technology the world reveals itself to us in a particular way: *as a resource well.* Nature and its objects and relations are

understood in this way. This perspective can be generally characterized in terms of a technological ontology, and science is the essential means at our disposal for understanding nature in this way.

4.5 Limitations of Modernist Approaches

In the debate between internalists and contextualists technological development is understood primarily, if not exclusively, in the context of design.

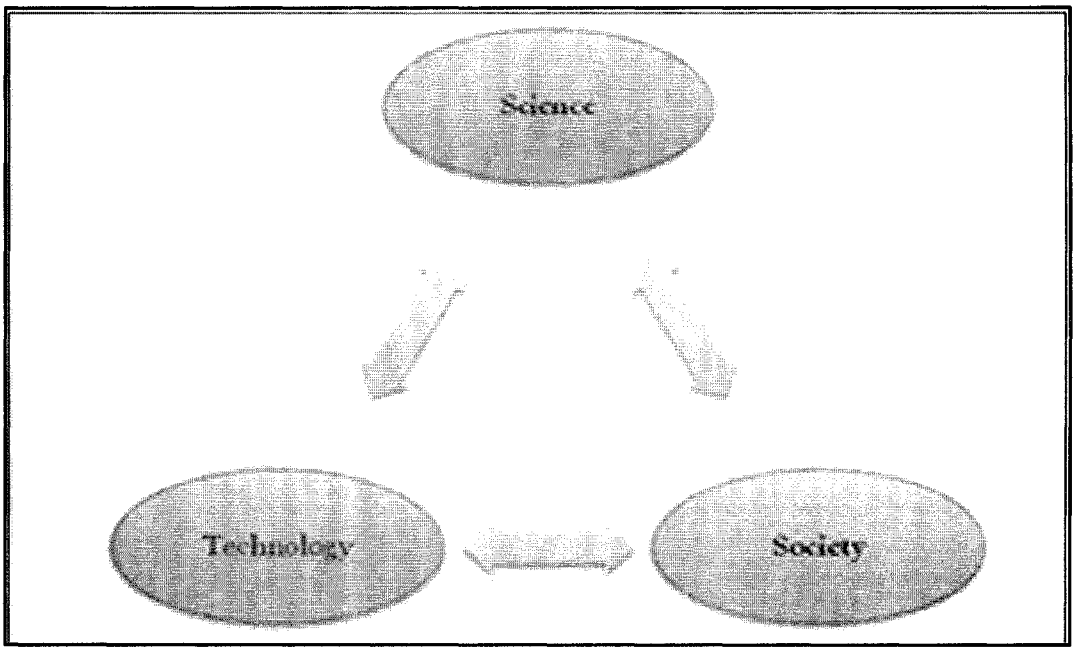

Figure 3: Spherical Conceptions Supporting Clear Separation

In the *interactionist* perspective, we see contexts of use emerge as important. Nonetheless, in all of the aforementioned theoretical traditions the essential logic of explanation is one which is predicated upon, and reproduces, the paradigmatic binary between people and things. While a full-blown meta-critique of these literatures is prohibitive in the current context, it is nonetheless necessary to call attention to the fact that the procedures associated with keeping to this

commitment are problematic where we are dealing with techno-social phenomena and techno-social systems. Indeed, investigations by other researchers have suggested that a distinct set of fault lines run through these literatures and that these fault lines derive from, and can be traced back to jurisdictional agreements between the natural and social sciences and the associated processes of accusation necessary to sustain them. Latour, in particular, has argued that when the orthodoxy of ontological dualism comes into

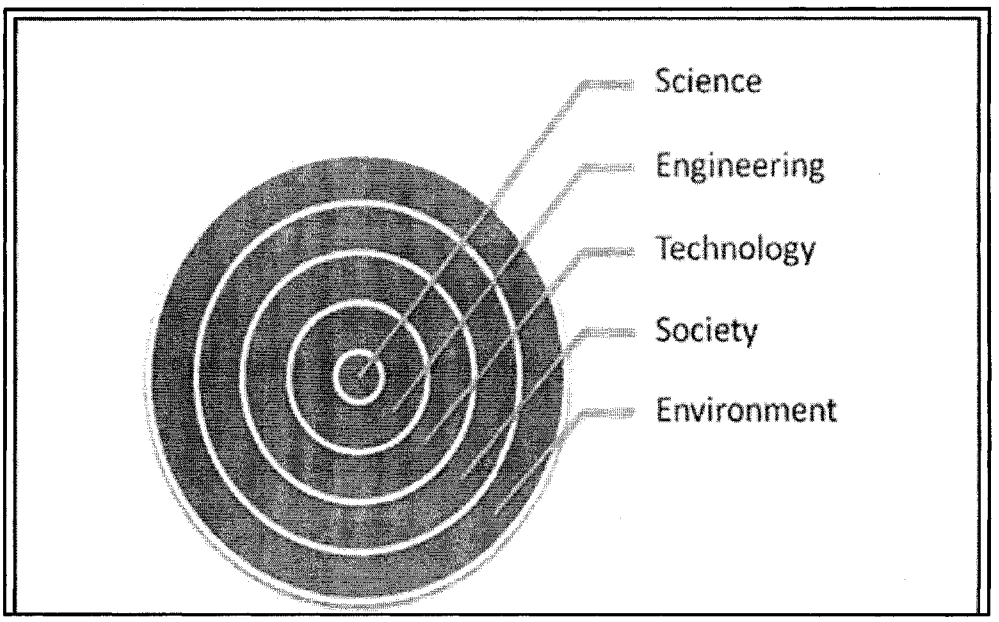

Figure 4: Concentric Models Based on Subsidiary Relationships

contact with technological object/systems (hybrids) what we see is a variety of explanative approaches based on forms of explanation which aim to separate out what is natural from what is cultural. Latour calls this procedure purification (1993).

When we examine the literatures on the Internet, several forms of such splitting for the purposes of purification are in evidence. Perhaps most the most

obvious of these lies in the employment of an explicit distinction between the Internet and cyberspace:[110] wherein the Internet is to nature what cyberspace is to culture[111] - or, to follow the language or Latour more closely, cyberspace can be treated as a space of pure sociality if the Internet, understood as 'the technology', is back-grounded and cyberspace is thereby purified of its connection to 'things'. Conversely, the Internet can be treated as pure technology, purified of its political and social properties[112] if these are back-grounded and the analytical emphasis is placed upon the circuitry and instrumentation. Just as often, however, it seems that the terms are used as though they are inter-changeable. On closer analysis, however, what we often see is that where the Internet is being treated from the standpoint of the social it is operationalized as environment/space inhabited by actors, ruled by norms and convention. And that, where the Internet is being addressed from the standpoint of its physical/technical structure, it is addressed as a system ruled by code. In the latter case the social origins of cyberspace disappear, while in the former case the 'nature like' limitations imposed by code disappear.

Whether one attributes the splitting within these discourses to a deeper set of tectonic tensions within modernist ontology or not, it should nonetheless be clear that they result in a historico-phenomenological failure at the level of reflexivity. By refusing to assume the separation between virtuality and reality as a given, I am not suggesting we ought to dismiss existing bodies of criminological

---

[110] A systematic study of the terminology is not here proposed.
[111] Where the Internet is the form (wires-hardware-software) and cyberspace is the content.
[112] This hardly shows up as terminological axiom

and legalistic literature that take cyberspace for granted. Nor is it my intent to deny that the distinction has any validity. My intention instead, as indicated earlier, is simply to insist that the persistence of this division needs to be understood as the ongoing outcome of social processes constructed and socially sustained, and hence that an examination of the positive processes associated with its ongoing social construction is wanting.[113]

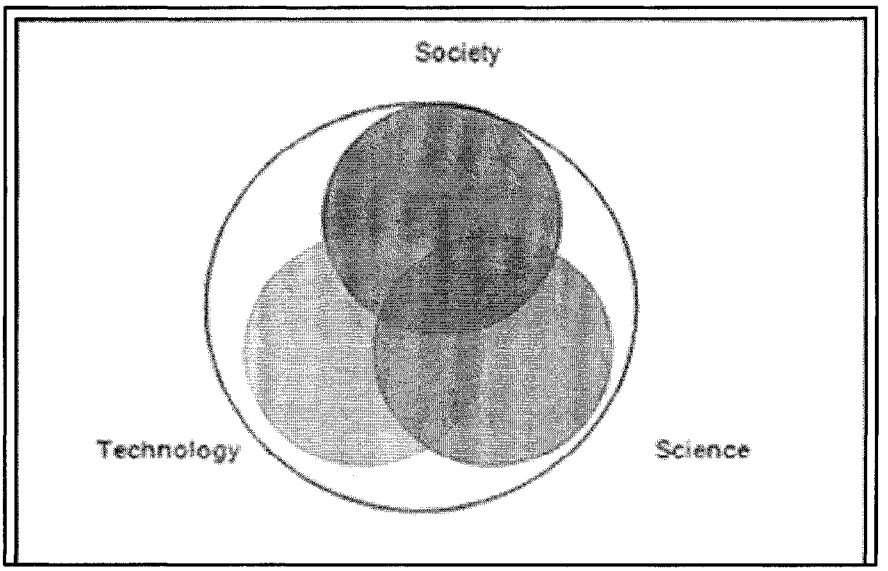

Figure 5: Venn Diagrams of Interpenetration

At this point I want to refer again to Foucault's conception of the event and eventalization. My aim in doing so is to try to restore the necessary horizon of reflexivity to analyses of the processes of problem solving associated with attempts to provide for the safety of children in cyberspace. My argument is that these problem solving processes must be understood stereoscopically – both

[113] The separation of virtuality and reality, of the online world from the real world involves a kind of purification, to follow Latour. Perhaps the best evidence of boundary maintenance in relation to such separation practices lies in the use 'spill over' language. We witness this in worries about whether a particular persons activities online are effecting their everyday behavior.

from the standpoint of the social processes involved in conceptualizing insecurity as a technical shortcoming which can be corrected through instrumentation, architecture or software – and from the standpoint of the social processes involved in constituting cyberspace as a secondary domain aimed at modifying the operating environment. This argument is developed in and through reference to the social construction of technology tradition.

4.6 Re-Sourcing Studies of Science and Technology

Around the beginning of the eighties, the 'science and society' movement came into confluence with the developing area of 'sociological studies of science in society' just as the later had adopted a 'strong program and the sociology of scientific knowledge' (SSK). Research in this area thus shifted from a functional understanding of science in society to a more reflexive examination of the culture of science and technology. The emergent commitment in the social construction of technology approach (SCOT) was to a position that would treat technological knowledge in the 'same symmetrical impartial manner that scientific facts are treated with within the sociology of science knowledge' (Bijker 2002). In this approach 'the success of an artifact is precisely what needs to be explained. For a sociological theory of technology, it should be the explanadum not the explanans' (Bijker 2002).

. The social construction of technology approach hence levels a significant critique against historiographic studies of technology. This latter field abounds with case studies which do not go beyond the context of the object they

investigate in order to link their historical trajectories to larger structural and systematic forces. In so far as these kinds of descriptive historiography do not link up with larger and more abstract social and system forces, the vast preponderance of them are 'asymmetrical' describing only the history of technologies that have succeeded, rather than those that have not. Such asymmetry functions to reinforce the view that technological development is linear, and that processes of 'technological development [...] followed an orderly rational path' (Bijker 2002). Social studies of science and technology show quite clearly that that there is no linear relationship between the discovery of scientific knowledge and subsequent technological development. Indeed, the desire to improve, expand or otherwise enhance the operation of a technological system is often the driving and directing force behind scientific research, steering the course of scientific inquiry and thereby structuring the pool of scientific knowledge.

Three concepts are central in the SCOT analytical toolbox and will be used in the subsequent investigation of processes of securitization. The first is the idea that technology is constructed by a variety of social groups. SCOT uses the 'term Relevant Social Groups (RSGs) to 'indicate such groups involved in the shaping of a given technology.[114] In the SCOT approach this means breaking out of the preconception that design decisions are made by engineers or that decisions are based on cost or efficiency. Second is the idea of interpretive

[114] 'An RSG can be any group, such as a company, regulatory agency, or consumers that defines, interprets and solves problems arising during the development of a technology (Kim and Watanabe 2001).

flexibility. According to this concept communities may be characterized by differing conceptions of the nature, potential and problems with an associated technology. In the event that there is a high degree of discensus the developmental path the technology is highly indeterminate. Finally, closure is conceptualized as a process involving as 'reaching agreements about which technological paths will be followed' (Williams 1999) and results in the acceptance of dominant solution and absence of strong alternatives' (Kim and Wantabee 2001).

In 2002, key proponents of the social construction of technology approach began to acknowledge that the political character of the processes associated with construction has been neglected. Indeed, they argued that technological cultures ought to be more explicitly linked to democratic politics, and that social construction of technology approach investigators ought to play a more prominent role as public intellectuals (Bijker 2002). To be more precise, the contention is that while it is important to continually emphasize the extent to which 'modern societies are constituted by science and technology, one cannot hope to understand them without taking into account the way that science and technology are constituted by modern society. SCOT must 'actively contribute to a politicizing of the technological by showing that 'science and technology are value-laden', that 'science and technology play key roles in keeping society together, and that they are equally central in all events that threaten its stability' (Bijker 2002). However, the 'normative, political or practical consequences of these insights' remained unaddressed. Thinkers working within the social

construction of technology approach therefore argued 'that societal problems urge a broadening of the science and technology studies agenda: 'the big issues of social order, international peace, local and social security, national and religious identity, and democracy should be addressed again, but now on the basis of detailed insights from the sociology of scientific knowledge (SSK) into scientific knowledge and technical machines' (Bijker 2002). The agenda can then move from studying the 'culture of science and technology to studying technological culture' (Bijker 2002).

4.7 Beyond S.C.O.T. - A Diacritical Model of Social Construction

Social Construction of Technology studies have also come under fire from outside by those advancing a social conflict perspective, for three key reasons. Firstly, social construction of technology approaches have been faulted for ignoring the fact that conflicts at the level of interpretation are ubiquitous and implying instead that interpretations are subject to a progressive process of convergence resulting in a working, if imperfect, consensus. Second, it neglects the role that power plays in determining which interpretations prevail and in accounting for the forms of stabilization that emerge as a result of what they describe as closure. It favours an over rationalistic understanding of the processes of technological development and also leaves the impression of linearity where in fact there is often confusion, chaos, and direct conflict. I find myself generally in support of the social conflict critique of the social construction of technology approach. It is clear that the key conceptual constellations

underlying the social construction of technology approach as a structure of explanation are underdeveloped and that the framework requires supplementation at both analytical and substantively. However, it is insufficient to simply say that conflicting interpretations, conflicting visions, and conflicting claims are the rule rather than the exception wherever a new technology or technological system is in the process of emergence, or even to insist that dissent, rather than consensus or consent, are involved. What is necessary instead is to understand the kinds of conflicts that are arise and what seems to be at stake. The aim of this section is thus to initially build upon but eventually advance beyond the social conflict critique of the social construction of technology approach in three ways. First, conflicts that emerge at the level of interpretation must be contextualized if they are rendered intelligible. We must have reflexive recourse to the broader background context of emergence (the ruling rationalities and risk logics at work within neo-liberal democracies). Second, it needs to be acknowledged that non-discursive modifications at the level of technological design and operation are subject to ongoing and parallel processes of interpretive contestation and that these may or may not be initiated in response to new interpretations. This is not a matter of saying that the Internet is gripped by this apparatus of power, but rather of saying that the network itself

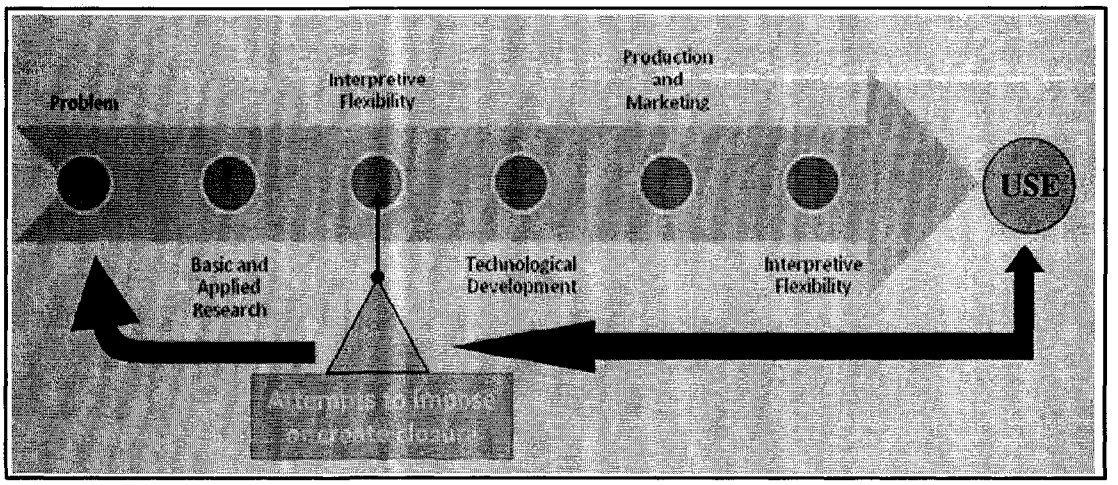

Figure 6: Social Construction of Technology Processes

is already an expression of that power and that its ongoing developmental processes need to be understood from the vantage point of neo-liberalism and of risk.

4.8 Synthesis: Toward an Analytical Framework

The SCOT model (Figure 8.0) demonstrates several shortcomings in relation to the Internet. First, it constructs design as a linear process and neglects the fact that where the Internet is concerned we are dealing with a far more dynamic system characterized by a complex interplay between discursive and non-discursive practices.[115] Perhaps more importantly, the processes of problem solving involved in action contexts invariably make reference to larger sets of political and economic background conditions, suppositions, and expectations. In order to conceptualize the processes associated with problem solving in relation

[115] Non-discursive practices might be described broadly as action upon action, and more specifically – in the socio-technical context, as the manipulation of matter in an effort to achieve an objective or outcome.

to the design of complex technological systems like the Internet, we need a more capacious and complex theoretical framework that links such processes to both the self-understandings and action orientations of actors in micro-theoretical contexts and to the larger sets of structuring logics associated with neo-liberal modes of governance and risk rationalities. Hence problem solving processes must be understood as a consequence both of: 1) the unique situational variables associated with action contexts, and 2) a broader set of background assumptions which both affect the availability of approaches to the interpretation of the prevailing problematic as well as the perception of the feasibility of solutions appropriate to its address and dispositions toward them. In relation to this last point, it is appropriate at this point to stress (lest my procedure from here on in be misunderstood as one of simply harvesting conceptual tools taken from SCOT and using them to analyze processes of securitization at the concrete level) that much of the groundwork necessary to make the modifications to the SCOT model proposed above, has already been laid. To be more precise, I have endeavored to provide some of the much needed exogenous political and socio-historical references points lamented as lacking in SCOT by providing an account of the development of securitization as a generalized imperative to the larger logics of risk and rationalities of rule characteristic of neo-liberalism. In this context, it will be recalled that my argument has been that an orientation toward securitization[116] (understood as a general mode of strategic action which aims to

[116] It should be recalled that securitization was in this context being distinguished from two other modes of strategic action: juridification and regulation. Juridification would have involved creating the conditions of possibility necessary to bring judicial power and criminal sanction to bear, and particularly creating the conditions of possibility for the

reduce or eliminate risk by addressing and acting upon its conditions of possibility) became the predominant mode of response to threats to children posed by cyber-pedophiles, cyber-pornographers and cyber-predators, and that the predominance of this definition of both the problem and the nature of its solution can be traced to structuring logics and rationalities associated with neo-liberal risk societies more generally. Furthermore, it should be stressed that a principal purpose of analyzing the representation of these threats by the media and in the market place was to shed light on the conditions associated with the emergence of the securing-child-safety-in-cyberspace problematic such that one did not have the impression of it having appeared out of nowhere and so that there would be some sense of continuity or link between these larger forums for claims making (media and market place) and the specific situational contexts of problem solving.

While the imperative orientation toward securitization contained in this problematic stands as a general back drop against which to interpret the activities of relevant social groups and the claims they make in processes of problem solving, it ought not to be understood as unambiguous or homogenizing. Indeed, dramatically differing conceptions of the character, quality and extent of risk and its sources may motivate radically different approaches to the social construction of 'security solutions'.

With these considerations in mind, I want to amend the model offered by the social construction of technology approach in order to reflect several insights

---

enforcement of the law. Regulation, on the other hand, would have involved the utilization of state administrative and executive controls conducive to steering at a distance.

based on the social conflict approach as well as broader structural considerations. The model for conceptualizing the processes associated with

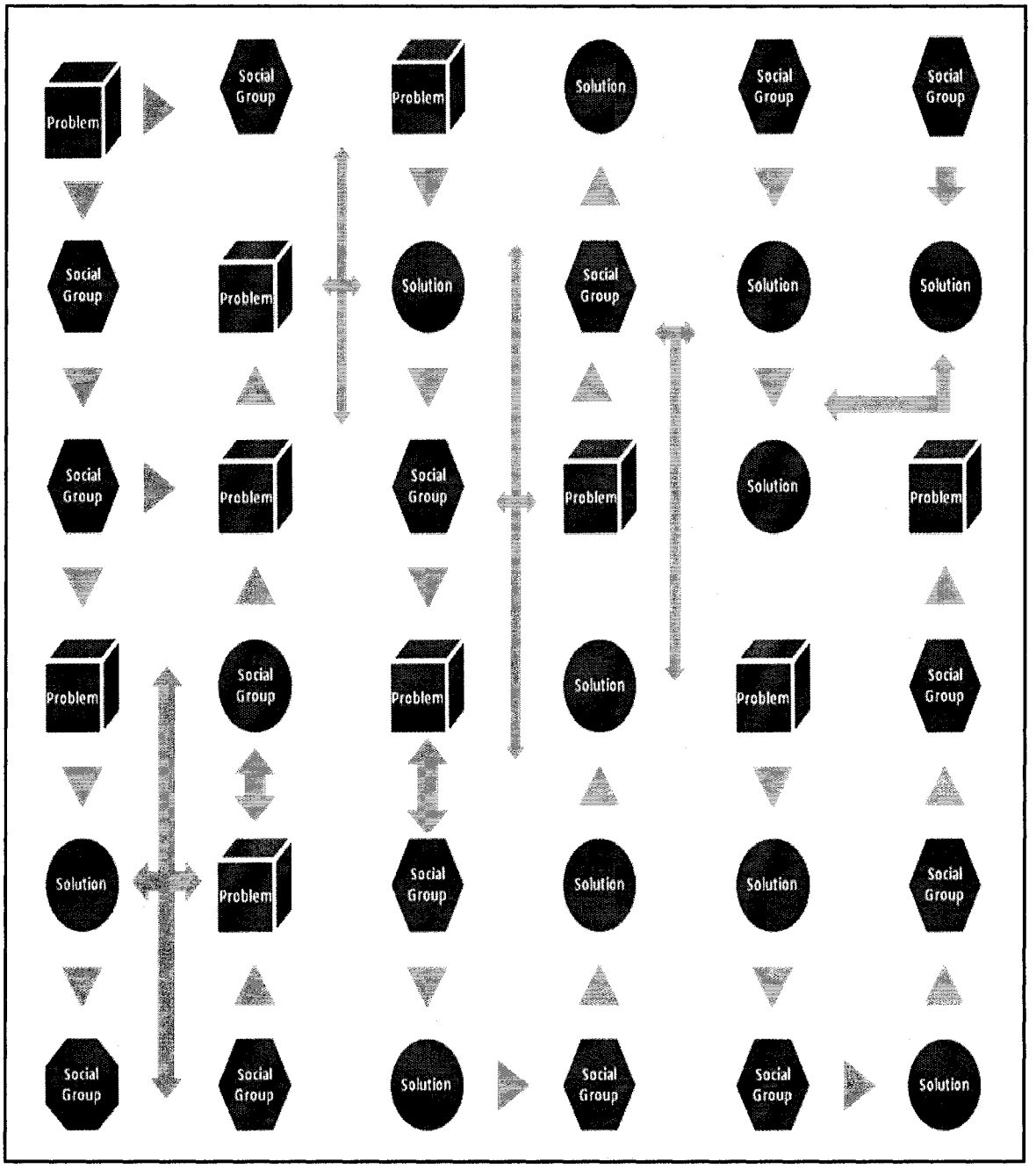

Figure 7: Revised Model for Conceptualizing Socio-Technical Processes

design according to the social construction of technology approach has been re-diagramed in order to reflect the complexity, contingency, and open-endedness

of these processes, as well as their changing and disjointed character on the one hand, and supplemented by the broader caveat that they are broadly oriented toward securitization on the other.

This model is beneficial in so far as it significantly expands the horizon of interpretive resources available in the analysis of processes of problem solving. First, it reflects the extent to which a variety of actors or agents, institutions and organizations ('groups' in the language of the social construction of technology approach) are involved in various processes of claims making with respect to problems and their solution. According to this understanding of the premises of the social construction of technology approach, the prevailing definition of a problem is understood and interpreted differently by different relevant response groups who are differently positioned to respond to it at the level of problem solving. Second, it not only allows for the activities engaged in by the relevant social groups identified by SCOT to be framed against the broader backdrop of the rationalities and logics characteristic of neo-liberal risks societies, but it also helps us to understand why some groups might become involved in processes of problem solving (and thereby become 'relevant') while others might not. Put differently, the very involvement of some groups, as well as their sense of identity and orientation, indicates that we are dealing with a problem which has (to a certain extent anyway) already been defined in a certain way. As will be seen subsequently, this is particularly clear in cases where third sector organizations and agencies have taken it upon themselves to become involved in activities like patrolling and policing the Internet.

4.9 Summation

This chapter assessed the strengths and shortcomings of existing approaches to the analysis of technological development and endeavored to develop a theoretical model with which to investigate the development of socio-technical solutions aimed at responding to the securing-the-safety-of-children-in-cyberspace problematic. It argued that any such framework must have recourse to both a macro-logical set of resources (which would help address why the security and safety of specific populations might become an ongoing concern and how systems forces and structural factors may influence the way a problem is both defined and responded to) and a micro-logical one (which can address how cognitive understandings may inform the behavior of actors). The SCOT approach was identified as a promising point of departure in the development of such an approach and several substantive modifications were proposed to address the models' shortcomings with respect to conceptualizing conflict as well as accounting for broader socio-historical factors and forces. The role played by the concept of securitization was identified as a key one in upcoming analysis in so far as it provided a broad frame of reference for the investigation and a more immediate vehicle with which to conceptualize the connection between situational features and structural forces.

Chapter Five:

Design Contexts: Securitization through Embedding

5.0 Introduction

In the tool-box of tactics used in pursuing securitization[117] as a general strategy, *embedding* is the most immediate in so far as it involves making physical, material or code alterations to virtual environments in order to remove or reduce conditions which are conducive to risk. The effects of this form of securitization are direct, relying neither on the consent of subjects nor on any recognition of their legitimacy for compliance. This chapter describes the players (relevant social groups) and processes (interpretive flexibility, contestation, closure) involved in the development of embedded approaches to securitization. It begins by describing and characterizing what is distinctive about embedding as a securitization strategy. Four approaches to embedding are subsequently identified, and the vicissitudes of each are examined in turn. Server-side approaches to embedding are the first to be examined. The second are full spectrum system-wide approaches. The third to be examined are end-user oriented or 'point of access' approaches. Finally, approaches based on sequestering or server segregation are examined.

---

[117] Recall that securitization has been defined as a strategy of risk management that aims to minimize, reduce, or entirely eliminate risk, primarily by addressing and/or acting directly upon its conditions of possibility. For example, since opportunities for loitering are said to be correlated with the risk of assault, and long benches where people can sleep are said to be correlated with loitering, removing long benches and putting metal chairs in their place has been adopted as a way of acting on one of the conditions of possibility of risk of assault.

The examination of each of these approaches showed that they were the subject of considerable contestation and controversy. I examine some of the relevant social groups (RSGs) involved and describe the character of their claims. The analysis shows that these group were engaged in addressing and attempting to resolve a variety of conflicts between 'security' on the one hand and freedom of access (or access to information) on the other. In other cases, the conflicts were between contrasting conceptions of what the nature of the security threats were, and thus how to address them to make children safe in cyberspace. To the extent that these debates foreground the political context and consequences of design decisions, I consider whether that they ought to be interpreted instances in the 'progressive democratization' of processes of design. In concluding this section, I link the findings of the chapter to the larger argument about the exigencies associated with governing children in neo-liberal forms of government. This is clear in the considerations which have had an impact on the emergence, reception, development, and adoption of these various approaches to addressing the problem of child safety in cyberspace. I argue that a constant theme throughout is the way that neo-liberal rationalities rely on civil society to organize and address itself to this issue. This is clear in a logic that delegates the market to develop technological solutions but allocates moral responsibility to parents.

5.1 Theoretical Preliminaries

At the onset of this investigation I indicated that I wanted to problematize, rather than presuppose, the separation between virtuality and reality, and proposed that a processual approach would better serve an investigation aimed at understanding cyberspace from the standpoint of its social construction. Part of the purpose of this approach was to counter the dematerializing tendency of hard constructivist approaches. In other words, it was necessary to acknowledge that changes in the properties of cyberspaces were linked to design contexts and that innovation and design changes have structuring effects which are relatively obdurate. In an effort to better conceptualize the impact of such processes in structuring the realities of virtual spaces, I referred to Lessig's (2000) designation of four types of constraints to regulate behavior: laws, social norms, markets and 'nature'. Lessig identified 'code' as the equivalent of nature in cyberspace. – or the software that makes cyberspace into 'a set of constraints on how one can behave' and concludes that code is the general, more pervasive and effective (immediate) constraint in cyberspace than is nature in real space[118]. Of course, in order to analyze comprehensively the options available to affect particular behaviors, all four types of constraints (and the potential of law to regulate via the other three) must be considered – this is why the current study looks at contexts of operation as well as contexts of emplacement.

Following Lianos with Douglas (2000), we can further ground the idea of code as 'structuring' in relation to what they describe as the emergence of

[118] However, code is more susceptible to being changed by law (more ductile or plastic) than is nature. Therefore, both code and law are more important as regulation of cyberspace than many realize or admit.

Automated Socio-Technical Environments (2000). For all intents and purposes, cyberspace is just such a techno-social environment though it is one that is only partly constituted by automated processes. The insight that cyberspace is design all the way down has led some thinkers to see it as a space of total control (Kroker 1996). However, the utility and explanative power of the social control paradigm as an analytical standpoint is questionable in this context. In part this is because it is a truism to say that decisions with respect to design are ultimately oriented toward social control simply because they are intended to either enable or constrain. Such an observation takes us no further forward in terms of understand the intentions underlying such decisions[119]. But it is also because there are a plurality of actors, entities and networks involved in design. Indeed, the overall architectural structure of the Internet is the ongoing outcome of decisions made in a variety of forums and contexts associated with governance including the World Wide Web Consortium, the Internet Engineering Task Force, the Internet Society, and the International Standards Organization. Governments are also involved in determining some of the structural and system properties through international agreements and a variety of treaties. The fluid nature of such structuration has led more than one theorist to suggest that we ought to conceptualize cyberspace in terms of a hydro-dynamic model of flows (Virilio 2001). This is not to argue, of course, that corporations have not increasingly become the controlling power and thereby gained greater impact on decision making with respect to infrastructure. However, acknowledging that some have

[119] Security may be enhanced through architectural design, but not all architectural design is oriented toward security enhancement.

more power than others over the design and development of cyberspace is a far cry from establishing it as a space of total control. We would be better off to acknowledge that elective affinities between different design communities may develop and/or dissolve in relation to certain strategic opportunities.

5.2 Automated Systems and Cyberspaces

This last caveat may seem to put us in an odd position in relation to the idea of automated socio-technical environments, because what Lianos and Douglas see as key to these systems is that their automated character cuts 'out negotiation [...] short-circuiting cognition and human value reproduction' (2000). This contention obviously cannot be sustained where cyberspace is concerned. Indeed, one of the defining features of cyberspace is its openness, plasticity and inclusiveness (Lessing 2000). This is not to say that 'anything goes' but simply that since it is a 'built' space, changes introduced at the level of infrastructure, hardware and code can introduce new behavioural possibilities as well as eliminating others. The democratic character of cyberspace has meant that a vast plurality of communities and individuals are involved in introducing such changes at various levels throughout the system. The open architecture of Internet protocols, the interoperability of platforms, accessibility to a diversity of programming languages, and the open retail of domains have made it possible for a plethora of individuals, organizations, institutions, corporations and countries to take part in the processes of structuring the Internet, both by contributing content and through coding, architecture and infrastructure. Some

argue that this openness and fluidity is precisely what is responsible for insecurity. To be sure, cyberspace is the site of an ongoing struggle between conflicting interests and, moreover, some insecurities are not accidental.[120] Market imperatives have both contributed to insecurity and responded to this insecurity by producing security solutions.[121] What is distinct and important for our purposes is that the case of the Internet is unique in so far as the sheer number of 'relevant social groups' involved in various levels of design and development is inordinate.

It seems important to concede, by implication, that there is no one 'cyberspace' but rather a plethora of cyberspaces that are the product of a variety of constraining and/or enabling actions executed at various levels of the system, some of which are attributable to other humans, some of which are attributable to software, some of which are attributable to fixed structure hardware, some of which are attributable to automation, and some of which are attributable to infrastructure. According to this understanding, the socio-technical structure of cyberspace at one point in the system need not be the same as at another. The content and contours of the space are an 'effect' of instrumental manipulations upstream and modifications at the level of the end-user downstream, and a product of actors and their activities within this techno-social environment. Information service providers, organizations, and institutions may make modifications in the way their systems operate upstream, and these may affect

---

[120] Thus with the emergence of malware and spyware – we have seen code that interferes with the ability of surfers to navigating their own course – hijacking browsers, and redirecting them to unintended sites.

the character and contours of cyberspace as a user environment 'downstream' – or schools and households may make 'terminal' or 'point of access' modifications to specific machines or networks which may modify (to varying extents) the cyberspaces that are accessible to them.

All of this has bearing, and is important if we take Lessig's proposition that code is the equivalent of nature in cyberspace seriously. It becomes even more so if we consider Langdon Winner's suggestion that technology also acts as a kind of legislation (1980). Changes to code can have the effect of altering, in a fairly fundamental way, the ontological character of cyberspace, but they are unlike law in so far as these alterations do not rely upon the willingness of agents to conform or obey. In cases where behavior is constrained by code, the spectrum of possibilities for disobedience is marginal (though not non-existent) and confined to the few who possess the technical savvy to circumvent the controls. It is also noteworthy that the logic of code and architecture is entirely different than the logic of law. Small changes at the level of code can have a system wide restructuring effect.

Having acknowledged that there are 'many legislators who are making laws' and that some such law making is deliberately aimed at exploiting pieces of legislation developed by others, it is easy to see why 'code' (understood as a form of legislation) has come into the realm of politics and been subject to much debate. Indeed, the hegemony of Microsoft has been challenged by open source products like Linux in a process of democratization in which technical solutions are increasingly subject to public scrutiny, and in which the validity of the claims

made with respect to products and practices is increasingly open to challenge. If we allow that it is accurate to conceptualize technical trajectories of development in relation to the Internet as the ongoing outcome of contributions of a plurality of different design communities, the question becomes which relevant social groups are devoting their efforts to developing security systems, and what countervailing forces are in evidence in terms of working on circumventing existing protocols and protections. We might use the Foucauldian metaphor of a struggle over the ontological character of cyberspace to describe the fundamental process of contestation. However, for the present purposes, the utility of the conflict perspective applied to the social construction of technology approach is clear and immediate, for here we find many cases of code war.[122]

5.3 Security as a Generalized Imperative vs. Securitizing Children

At this phase of the analysis we might do well to distinguish forms of embedding that aim at securing children and embedding in terms of the larger context of invention, innovation and design. In a certain sense, security as a generalized imperative at the level of systems development and design is indivisible from the imperative to securitize children. Efforts in the first respect are bound to impact on the second, and the second will not likely succeed if the first are not sound. In the context of the current investigation, however, it is important

---

[122]The origin of this term is not certain. However, it is used to refer to cases on the Internet where conflicts over values become embodied in software. Pieces of software are hence written to combat other pieces of software. A classic example is the case of 'Circumventor'. This software application is designed to thwart all filtering and blocking programs.
http://www.peacefire.org/circumventor/simple-circumventor-instructions.html

to note that while we are interested the development of embedded approaches to securitization, where we are talking about the overall processes of design and modification associated with the Internet, 'security' is only one consideration or 'value' amongst many others that may enter into play in the processes of design and development. It is hence important to distinguish between general contexts wherein security issues are only one consideration that arises in the design and development of hardware, software, networks, and particular applications or websites, *and dedicated design contexts* wherein the primary aim is to address, rectify and or eliminate insecurities by developing a product, architecture or space that will enhance security. A full blown discussion of the former, broader context, in which security considerations have entered into and influenced hardware design, network design or operating and network systems[123] is beyond the scope of the current inquiry.[124] However, some elementary illustrative examples may be of service so that the distinction between these kinds of activities is clear.

One of the primary ways that the security of users has been operationalized at a more general level is in terms of the security of information. This is reflected in more concrete concerns about privacy and identity, and more particularly about the potential that embedded forms of surveillance have to

---

[123] At the level of a given network, or of a specific service provider, it is important to note that systems security and personal security are connected. A compromised system may result in threats to the security of all of its users.

[124] An ethnographic study of the role and import of security concerns in the overall design process is not contemplated here. Such a study would need to consider software and hardware engineering contexts, as well as system of information service providers.

interfere with privacy by collecting and disseminating information about users that they have not authorized or consented to share. While such cases are not specifically about the security of children, but reflect a more general concern about the security of the population, it is quite clear that children are just as affected by embedded forms of surveillance as everyone else is. *Cookies* provide a good illustration of how decisions taken at the level of network and architecture design can have an impact on security at the level of the Internet as a system. Cookies first appeared with Netscape Navigator 2.0 – and can essentially be understood as surveillance systems that make use of use Internet protocols, server side software and users browsers to allow for the placement of information on a user's computer and its subsequent retrieval at a later date. This information indicates whether and how often a particular user has visited a site, and may well indicate a great deal more including other sites the user has visited, and personal information. Before the use of cookies was problematized, their use first had to be detected and their modus operandi identified. Subsequently they came to be seen as an infringement on privacy[125]. When their use was subsequently brought to public attention and problematized – users were then given a notice that a cookie would be installed on their system. They then had a choice as to whether they would accept the cookie and be allowed to view the site or reject the cookie and not be allowed to view the site. There was no opting out option (Greenleaf

[125] There is a growing body of literature on this issue. Some good starting points include: DeCew, Judith. 1997. In Pursuit of Privacy: Law, Ethics, and the Rise of Technology. Ithaca, London: Cornell University Press. Whitaker, Reg. 1999. The End of Privacy: How Total Surveillance is Becoming a Reality. NY: The New Press and Agre Philip and Marc Rotenberg (Eds.). 1997. Technology and Privacy: The New Landscape. Cambridge, MA: MIT Press.

2003). In subsequent browser designs, this privacy issue was addressed. The point of this is that host servers are configured to recognize cookies and that this process of recognition is only possible because the Internet protocols provide for it. Security, or the lack of it in this case, is a consequence of design at those two levels.

Security considerations may come to occupy a prominent place in terms of the overall design and development of operating systems. Microsoft, for example, in developing its XP operating system, has been plagued by security flaws, some of which have allowed systems to be hijacked and commandeered for illicit or illegal uses. Hence, the company is constantly forced to provide 'hot fixes'[126] and to issue security notices.[127] However, although security was a consideration in the design and development of XP, the purpose of XP is to provide an operating environment which will allow the user to run other applications.

Security options may also be designed into an application whose primary function is not security. As an example in this case, the primary purpose of Internet Explorer (IE) is to allow users to browse the web. However, some security features are also designed directly into IE that allows users to control the kind of content the browser will display, as well as to set their desired level of privacy. High privacy settings may result in denial of cookie installations – resulting in the inability to view particular pages. High security settings may result

---

[126] The term is used to refer to modifications to code that can be added while the application is running and without requiring the user to shut down and restart the system.
[127] The effect of these notices on users overall feeling of safety is not investigated here – but it hardly needs to be pointed out that Microsoft supporting products are programmed to display alarms when they detect that a system is not running with the latest security fixes.

in access to pages with profane or 'inappropriate' content being denied. In the context of e-mail and chat applications, some obvious developments were introduced which have been of benefit to children though they were not specifically introduced for them. An example of this is that children can place unwanted email senders on a blocked senders list. Similarly, children in chat rooms can block other occupants and place them on a no-chat list. In other words, we have seen some modifications at the level of design that may substantially lessen the likelihood that a child will be exposed to unwanted attention. Given these examples, let us now turn to an examination of securitization in the context of *dedicated design*.

5.4 Server-Side Embedding and Information Service Providers

One of the proposed approaches to securitization using embedding that arose early in the period under examination was server-side embedding. Such an approach involves tasking or requiring that ISPs filter out content and block access to sites determined to be unacceptable up-stream. In the Canadian context this approach was subject to considerable investigation and discussion. After a series of studies, including the influential '*Regulation of the Internet: A Technological Perspective*' the Government determined it would not undertake to require service providers to try to control Internet content at the level of the network. Several reasons for such a decision were stipulated including cost, performance and efficacy. In addition, however, there was a prevalent perception that taking such action could hinder other *Charter* values including freedom of

expression – and that it might also hamper the ideal of the Internet as a forum for the free expression of ideas. The position adopted by Industry Canada and the Association of Internet Service Providers in relation to this issue is noteworthy. Both organizations draw a distinction between offensive content and/or conduct and illegal content/conduct. The latter is held to be the purview of law enforcement, although it is acknowledged that steps can be taken by service providers to lessen the likelihood of such content or conduct. General worries about 'censorship creep' also played a role in so far as filtering at the level of the ISP might make content susceptible to further encroachments on freedom of expression, particularly in so far as it would provide governments with a vehicle or target. A number of technical solutions were proposed and examined, but the 'Internet Access Controls without Censorship' model came to be adopted with an emphasis on a multiplicity of rating systems, voluntary self-rating by content providers and blocking software on home computers. What is important to note about the construction of these individualizing approaches to risk management through securitization is that they were conceived as 'no penalty' forms of risk management, in so far as they are targeted to minimize, reduce or eliminate potential hazards to 'at-risk' populations but would involve no loss or cost to those who were never at risk.

On the basis of the foregoing discussion we might justifiably conclude that there was clear closure around this issue i.e., agreement that server-side embedding was not a path that ought to be followed (Williams 1999) and that such closure was predicated on the conviction that risks associated with harmful

conduct and content could best be addressed elsewhere thereby protecting freedom on the Internet and allowing the market to steer the course of innovation. The insight provided by the social construction of technology approach is helpful in this context, since it stipulates that such closure need not be not decisive. Indeed, while there is a general tendency for closure to be irreversible, reversibility is conceptualized as inversely proportionate to the degree of interpretative

flexibility.

In fact, in recent years the question of the viability of server-side embedding has re-surfaced. In this context, Zittran has argued that early efforts to control the Internet focused on the endpoints of the network to the determinant of giving full consideration to the potential of ISPs as sources of control (2003).Indeed, he goes on to contend that the potential for ISPs to play a role in regulating content at the ISP source can no longer be ignored:

> Internet service providers can serve as Net police, not only cordoning off areas from view when acting as hosts of content, but also more broadly restricting access to particular net-worked entities with whom their customers wish to communicate, thus determining what those customers can see, wherever it might be online. The publishers, themselves no strangers to creative and cutting-edge (if so far somewhat hapless) approaches to taming the Net, are no doubt watching closely, and will endeavor to adapt this sort of progress on anti-pornography, should it succeed, for use in their own battles (2003).

Notwithstanding such contestation however (and without putting too fine a point on it) there is clear evidence in these discussions and debates that the problem of securing children in cyberspace came to be generally regarded as one which could best be met at the terminus, reception end, or desktop. In this

context, a variety of problem solving strategies aimed at entrenching protection and prevention measures into the very fabric of cyberspace emerged. One involved the construction of a standardized and globalized content rating system, another involved building and embedding automated machines which would prevent children from being exposed to harmful or illegal content/conduct, and a third involved creating 'gated communities'.

5.5 Mapping the Moral Content of Cyberspace

One of the means of reducing and managing risk is to quantify it and isolate its characteristics spatially. Just as the governmentalization of the state mobilized cartographic resources to map its territory and spaces, and just as such mapping involved the concomitant emplacement of sign posts to designate places and distances, efforts aimed at the securitization of cyberspace gave rise to a new kind of cartography. Rather than relying on a legend that represents spatial coordinates in relation to true north, in the case of cyberspace the mapping processes relied on a moral compass. The construction of standardized categories for the classification of content was a solution that emerged in response and resistance to the Communications Decency Act in the United States, and was an alternative approach to governing the security of children in cyberspace. Such rating systems would rely on a secondary subscription to a service or on a software package which would provide access to the ratings and allow parents to set up their own customized control.

The self-identified purpose of filtering as a solution which relies on rating systems is to reduce or outright eliminate the risk that children who are surfing the Internet may come into contact with harmful content or conduct. Filtering software may work by examining the content of web pages that a browser is attempting to access against a master list of words and phrases, and/or by relying upon rating systems to determine whether the content the browser is trying to access is acceptable. The functionality of these programs has been called into question for a number of reasons, including that many websites do not have any ratings and are often summarily blocked. Critics have also charged that these systems effectively remove debates about values from the public sphere, in so far as the matter of developing specific criteria for classification, quantification and standardization becomes entirely technical. Normative judgments are made routine and automated in this process.

In this section I consider two of the schemes for the classification and rating of content. In the North American context these are the Recreational Software Advisory Council on the Internet (RSACi) and SafeSurf. Both of these rely on the broader standards and specifications set out by Platform for Internet Content Selection (PICS) specifications.[128] These systems largely rely on web sites to do their own rating, but this process has been very slow. What is of

[128] SafeSurf joined a number of others in the PICS alliance including: Apple Computer, AT&T, America Online, Center for Democracy and Technology (CDT), CompuServe, IBM, IHPEG, Information Technology Association of America (ITAA), Interactive Services Association (ISA), MCI, Microsoft, MIT/W3C, Netscape Communications, Open Market, Prodigy Services Company, Spyglass, Surf-Watch Software, Time Warner, and Viacom. The processes associated with the development of PICS are attributable to the work of technical experts operating under the auspices of the World Wide Web consortium. A special technical subcommittee of on PICS was created in 1995 and oversaw the overall development of the Platform for Internet Content Selection.

interest in terms of embedding as a logic of risk management, however, is that the development of these standardized rating systems allows for a very specific operationalization and quantification of risks. This is so to the extent that these systems actually have ratings that distinguish between different age groups of children. All of this is enabled by the development of PICS. According to the World Wide Web consortium:

> PICS is a mechanism for communicating ratings of web pages from a server to clients; these ratings, or *rating labels*, contain information about the content of web pages: for example, whether a particular page contains a peer-reviewed research article, or was authored by an accredited researcher, or contains sex, nudity, violence, foul language etc. Instead of being a fixed set of criteria, PICS introduced a general mechanism for creating *rating systems*. Different organizations could rate content based on their own objectives and values, and users - for example, parents worried about their children's web usage - could set their browser to filter out any web pages not matching their own criteria. Development of PICS was motivated by the anticipation of restrictions on the Internet such as some recent US legislation (the Communications Decency Act and its subsequent overruling by the Federal Supreme Court). PICS is a restricted metadata framework. It allows certain things to be expressed very precisely about web pages; in particular, PICS is useful when all the possible data values can be known in advance.[129]

Although both systems remain operational, I have chosen to focus my primary analysis on SafeSurf. In part this is because it was one of the prime movers in the drive to develop the PICS system.[130] For the purposes of this discussion I will highlight some of the key moments in the development of SafeSurf and subsequently describe their online content classification system. My aim will be to show how SafeSurf constructs the security solution it offers in relation to the

---

[129] http://www.w3.org/TR/NOTE-rdf-simple-intro-971113.html

[130] In their 1995 press release *SafeSurf* outlined the idea of PICS as a plan to 'save the Internet'

threat it deems present – and to show how it aims to empower parents through rating and standardization.

According to its website, SafeSurf was founded in 1995 out of concern for children 'accessing adult material and the potential trauma associated with early exposure to pornography'. Safe Surf's explicit purpose is to 'protect the innocence of children'. The groups founding members represent a wide range of constituencies, but clear connections to the neo-conservative right in the United States are apparent. Several of the group's founders are signatories to the 'Declaration of an Independent Cyberspace', others are members of the 'Founders of America' organization, including the President of the organization.[131] The organization boasts having received a number of awards including the Blue Planet Award[132], The Skylight Award of Excellence[133], and the World Technology Award – Ethics Fellowship.[134] SafeSurf bases its activities directly on the 'Declaration of An Independent Internet':

> We hold these truths to be self-evident, that all lawful information is created equal, that this information is endowed by its creator with certain inalienable rights that among these is the right to be distributed via the Internet without governmental censorship. That whenever any legislation becomes destructive of these ends, it is the duty of the members of the Internet to oppose it, and to institute self-regulation with parental control, laying its foundation on such principles and organizing its powers in such form, as to them shall seem most likely to effect the safety of children and the sanctity of distribution.

We can learn much about the way the security needs of children are constructed from an analysis of SafeSurf materials. First off, the organization takes a

---

[131] http://home.earthlink.net/~forfreedom/index.html
[132] http://www.af-info.or.jp/eng/honor/honor-e.html
[133] http://www.martinr.com/awards/award075.html
[134] http://www.wtn.net/awards.html

definitive position against government involvement in the Internet – arguing that such actions would not and cannot protect children, but rather would be harmful to them, in so far as they would create a fear of information and a fear of government. Indeed, government censorship is described as 'dangerous', because it has been misused in the past for the purposes of social control. According to SafeSurf, governments have used such powers to constrain someone who is 'not cooperating with its master vision'. This power is also linked to 'despotism'.[135]

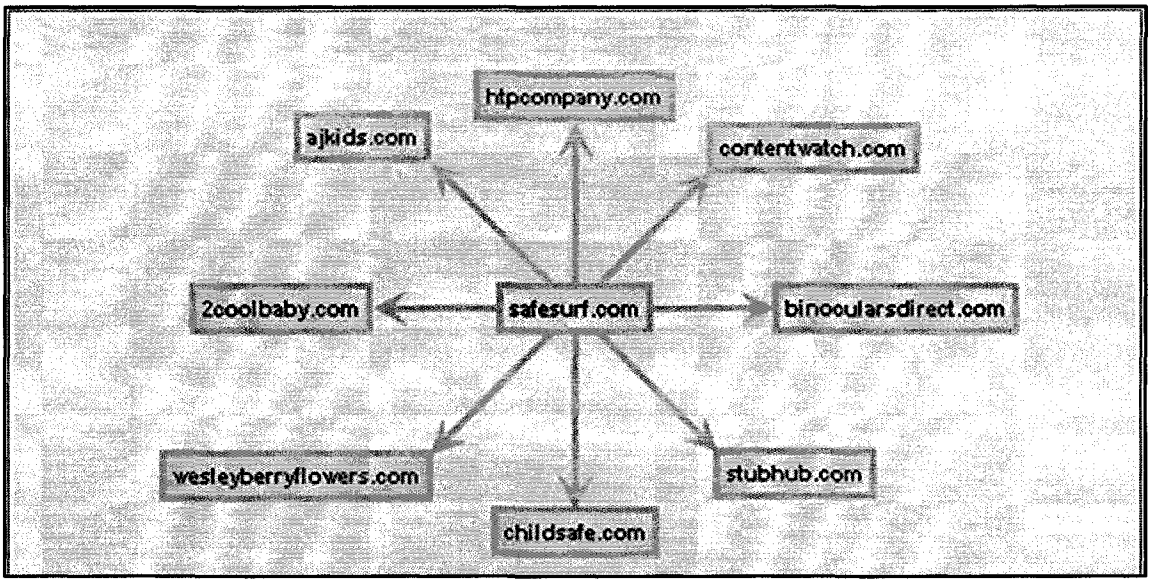

Figure 8: Diagram of SafeSurf Affiliates

The SafeSurf Rating Standard is constructed in contrast as a voluntary rating system designed to protect children, as well as the first amendment rights of their parents. The operators of SafeSurf also reject the involvement of government on the grounds that such involvement is 'uniformed', 'panicked', and 'over broad'.

[135] This allegation or worry may now seem a little less absurd given recent developments in China. To be more specific, the government of China has adopted censorship as an approach to addressing content it determines to be dangerous and/or threatening (Geist 2003:143).

The operators also enshrine 'prudence as the dictating principle with respect to content decisions'.[136]

The organization's opposition to government involvement is also based on the claim that government intervention will not prove efficacious, as 'the government decides what is indecent, but it may not match your standard'. As a server based solution, SafeSurf asserts that it can meet the moral needs of parents with different standards and viewpoints through its filtering and complex rating grid. The organization does not retail software, although it does offer assistance to filtering companies. Sites may opt to self-regulate, and having done so, may then download a logo to place on their page. Raters may rate pages individually, or rate the whole site. SafeSurf sees itself as distinct, indeed better than RSACi for two reasons: SafeSurf explicitly embraces the openness of the Internet, but asserts that a simple rating system is insufficient to deal with the kind of diversity that is emerging there and SafeSurf's detail insures that a self-rating publisher with a unique document has enough descriptors available to describe his content without branding it. The latter is accomplished in three ways. 'First, it is more detailed. Second, its goal is to objectively describe both content and how that content is presented. Third, it is the first system designed to allow

---

[136] 'Prudence, indeed, will dictate that regulations long established should not be changed for light and transient causes; and accordingly all experience hath shown, that mankind are more disposed to accept censorship where none is required, than to right things by opposing such censorship. But when an unnecessary attempt at censorship, pursuing centralized control evinces a design to place information under absolute Despotism, it is the right of the members of the Internet, it is their duty, to oppose such legislation, and to promote self-regulation with parental control' (http://www.safesurf.com/ssindep.htm).

those who self-rate and those who evaluate to have enough flexibility to reach an accord on a rating without compromising'.[137]

5.6 The Codification of Judgment and Embedded Actants

The level of codification and extent of judgment required to rate a site or individual pages according to the SafeSurf system is quite extensive. SafeSurf copyrighted this codification system which is developed around the core principle of assigning adult themes and caution levels. Nine different cohorts of ages are identified. In addition to this indicator of age, the content of sites or pages is rated according to nine individual considerations including profanity, heterosexual themes, homosexual themes, nudity, violence, intolerance, glorifying drug use, gambling, and other adult themes.

One of the most remarkable event-moments in the history of the development of the Internet has been the design and implementation of autonomous automated censoring machines (AACMs). When these programs designed to provide security are running, they form part of the operating environment and thus constitute actants. That is to say, in another way, that they move into the embedded area. As an analogy at the physical level we might be tempted to think of locks on doors that keep certain populations out, but the effect of actants is more extensive than that. These machines have the status of actants in so far as they constitute part of a security-surveillance network and, in so far as what they automate is a normative judgment, they have the status of moral actants. It should come as no surprise then, that the development and

[137] In June, 2004 the United States Supreme Court found that filtering and blocking solutions were preferable to the Child Online Protection Act (COPA).

deployment of these 'machines' has been the subject of a great deal of controversy and debate. What we find when we examine these debates is especially informative when we think about the politicization and democratization of design. On the one hand, we have a series of objections about censorship as a practice – objections that certainly make sense in terms of our neo-liberal *mise-en–scene* and in terms of the broader libertarian ethos of the Internet. But what we also see is a series of more specific debates around the efficacy of the design of these machines – and around the very definition of security that informs their construction. I will begin by sketching the general context of debate around the emergence of censorware – and subsequently will look at debates about their efficacy in relation to Internalist approaches to the explanation of technological development. Then I will look at the more general discussion around security and what security means in the context of these debates.

Although these devices were initially hailed as user-end oriented security solutions that would protect children from inappropriate content and/or conduct and illegal content/conduct while still safeguarding freedom of expression on the Internet, their implementation brought about a politicization process in relation to the freedom of speech. Many of the concerns in this context were not addressed to children as an at risk population per se, but to the idea that these technologies might have a slippery slope effect – 'allow a little censorship and eventually the whole net is open for redaction'. In fact, subsequent development has borne out these reservations in a variety of contexts.[138] What is at issue in terms of the

[138] Just recently, Microsoft has implemented a 'bot' that detects profanity on its blog sites and removes it (http://groups.msn.com/Script-BotTests/codeofconduct.msnw).

overall design of the Internet in this context is whether concerns about security for children should be allowed to trump free speech.

The efficacy of these systems has been a central issue of dispute. It will be recalled that in the fourth chapter we saw that the split between two traditions in accounting for trajectories of technological development, the Internalist (according to which the direction of technological development is largely endogenous, determined by the autonomous logic of scientific discovery) and the contextualist, (according to which larger economic, political and social conditions determine the direction of technological development) had eventually given way to a series of approaches which emphasized interaction. In the design and development of filtering solutions we see this debate resurface in significant ways. On the one hand, these technologies ostensibly emerged in response to public demand and thus their emergence is explicable in terms of a contextualist approach. On the other hand, their functionality proves to be quite limited, and it is limited both by the existing reservoir of scientific knowledge, and by the constraints of the growth rate of the Internet. To be more precise, much of the criticism of these approaches has focussed on the fact that the processes whereby they build blocking lists are themselves automated, relying on 'search bots' which troll the Internet looking for key words in order to identify content that is subsequently deemed inappropriate, adding the URLs of found websites to a list that is not even subject to subsequent validation. In some cases, blocking companies have resorted to concealing the sites that they have blacklisted with

the explanation that this is to prevent their competitors from piggybacking off their work.

What is under attack here is not the notion that we should protect children from harmful content but the how or processes whereby we can protect children from harmful content by blocking their access to specific sites. What is in dispute here is not the end, but the means. This is what establishes these as disputes of design. The Internet has spawned a variety of initiatives aimed at challenging the claims made by blocking and filtering companies.[139] While it is tempting to interpret the activities of these organizations in terms of a Foucauldian motif of resistance, it may be more fruitful to think of such disputes using a Habermasian speech act perspective taken from the *Theory of Communicative Action* (1987). To be more precise, what we seem to have in cases of opposition to censorware is both a challenge to the validity of the claims they make in relation to the functional efficacy of their products and a more general challenge to the very idea that censorware is the right choice to make in terms of protecting children from inappropriate or harmful conduct online.

Debates about the efficacy of filtering and blocking software have also led to a more general politicization of design in relation to security. One of the themes that has emerged is that security is not something that can be effectively addressed by technology at all. In media contexts this is seen in the recurring motif that discretionary judgments must invariably be involved when children are surfing in cyberspace and that technology is no solution for parental supervision.

---

[139] Perhaps the most renowned of these is *Project Censorware*. Founded in 1997 – the organization has devoted itself to exposing the short comings of blocking solutions in particular – insisting that it should be based on accuracy and should not be overbroad.

We have seen that the struggle over censorware resulted in a general process of the politicization of design, but what we also see is a developing recognition within these debates and amongst participants that the design is not neutral – that they have a social impact. We could speculate that this is because the electronic commons is something that is wholly built and thus a reflexive awareness of how, in a certain sense, our inventions reflect us has been fostered.

5.7 Gated Communities

The founders of America Online began Quantum Link in 1985. The company dissolved in 1991 and changed its name to AOL. Since that time it has marketed itself as a family friendly Internet environment, and a secure way for children to get online so that they can enjoy the benefits of Internet access within an environment that is subject to much more control than otherwise would be possible. AOL is the largest Internet company in the world. In 1999, it bought Netscape. For a five year period between 1998 and 2003 most computers came prepackaged with AOL. AOL has been hailed as one of the safest places online for kids by many media sources and technology experts.

Understood as a gated community, AOL consists of both family suitable content in its larger Intranet[140] environment and a whole special Intranet cyberspace devoted to children called KOL – or Kids On-Line. In this analysis I

[140] An Intranet is a private network that operates using Internet protocols and standards. It may be accessible through the Internet but has typically has more tightly controlled access restrictions.

will first address the environment created in the KOL and subsequently move on to discuss the way security is governed on AOL more broadly.

KOL can best be conceptualized as a maximum security environment. The means through which this objective is achieved are manifold. First, the space itself is segregated from the rest of the Internet. Child users may not leave AOL unless they have been granted permission to do so. Those who do want to leave the safe gated space of AOL are warned prior to leaving that in doing so they will not be under AOL's protective watch. Analogously, no one who is not an AOL member may enter AOL space. This means, at least theoretically, that AOL has hermetic control in terms of authorizing people to enter its space and determining who is allowed to remain. This power alone contrasts greatly with the situation of the Internet writ large, wherein users who lose access to the Internet from one ISP may simply seek out another service provider.

As a second securitization measure, all of the content on KOL (except the message board and chat forums) is subject to systematic development, review and oversight. Further, to ensure the security of the message boards and chat forums, AOL keeps in its service approximately 10,000 volunteers who function in various roles (Group Leaders, Community Leaders, Rangers, and Administrators) and assume a wide range of responsibilities in terms of monitoring and sanitizing the space[141]. This includes making sure that users adhere to a strict code of speech and behavior, recommending sanctions when they do not, and ensuring that all members are advised of and comply with the

[141] These volunteers receive free access in exchange. I shall not go into too much discussion of these monitors here – as their activities are more properly understood in the context if operations.

terms. In addition to these environmental controls, KOL has its own specific search engine that has been pre-rated and is guaranteed to deliver age appropriate content.

As if these server side cyberspace modifications were not enough, AOL and KOL both have their own tailor made browsers so that security is built even more deeply into the system through redundancy. The parental controls provided by AOL are among the most extensive in the field. The assemblage is one of total surveillance including monitoring and reporting on Web browsing, monitoring, logging and censoring instant messaging and online chats, a time clock system to track use, a log system of applications and sites visited, and finally, a guardian which accompanies children who surf and reports inappropriate activity to parents through email or instant messaging. The parental control functions allow for a good deal of specificity: parents may adjust the setting to different age groups: 3-5, 6-8, 9-12.

Given the totalizing measures that AOL and KOL bring to protecting children in cyberspace, it should be clear that the vision of security that they ascribe to is primarily one based on isolation and the containment of threats through a fortress-like mentality. The innocence of children and their need for full protections is paramount. While the literature on the growth of gated communities in the United States may provide further direction in terms of exploring the impact and implications of this approach to security, some initial comments on the insecurity/security dialectic may be in order here. First off, the explicitly privatized nature of AOL and KOL has meant that there have been repeated and glaring

problems in terms of the exercise of coercive power and abuses of authority. The emphasis some volunteers place on adherence to the Terms of Service and speech code has resulted in uprisings both in the AOL community and in the formation of a number of sites and UseNet groups devoted to a critique of their practices.

Perhaps most significant in terms of embedding is that AOL routinely engages in deleting entire threads of content or closing down chat rooms and other venues that it determines offensive or inappropriate. The power of code here – and of infrastructure – to enact definitions of security is quite clear in these cases. In a related matter, the perception that AOL is engaging in practices that are contrary to the spirit of the Internet has meant that it has become a favorite target of hackers and is often a target of exploits. As a consequence, AOL security has repeatedly been compromised and vulnerabilities have been published across the Web that has subsequently been utilized for the purposes of disseminating malware and spamming children with pornography.

5.8 Summation

This chapter identified four forms of embedding: up-stream or server-side embedding, globally located opt–in embedding, software specific end-point embedding and embedding by sequestered server. The analysis showed economic considerations and concerns about freedom of expression caused governments and service providers to reject the tactic of upstream embedding. While the use of filtering systems was favored instead, the foregoing analysis

showed that the development of such systems has not proceeded without controversy and the questions continue to persist about both the efficacy of such systems overall and the validity of their systems of classification. Finally, the description of gated virtual communities showed that a very high level of security was envisioned as attainable by maximizing surveillance, monitoring, and policing.

Chapter Six:

Contexts of Operation: Interveners and Intermediaries

6.0 Introduction

Chapter Three linked representations of threats to children in cyberspace found in the newspaper media and extant in market-place advertising with the broader structuring logics characteristic of neoliberal risk societies. It argued that the effect of these structuring logics was a general disposition to frame and present these issues as risks that could be managed, and that (as a result) the problematic of securing-child-safety-in-cyberspace became the dominant way of thinking about and approaching these issues. Two features of this problematic were identified as critical; it operationalized the problem as one of security, and this had the effect of drawing in a much broader spectrum of actors and of making the imperative actionable across a broader spectrum of contexts. Chapter Five explored the way that this problematic was taken up and responded to in design contexts, described the development of strategies aimed at embedding security, and showed how these were subject to various processes of contestation, politicization and democratization. For example, while standardized rating systems were developed in order to make a variety of filtering and blocking options available to children and parents interested in safely navigating cyberspace, the substratum of normalizing judgments underlying such rating systems were subject to considerable controversy.

In this chapter the focus is on securitization strategies that aim to curtail harmful, inappropriate, dangerous and illegal conduct and content in cyberspace by means of direct intervention and intermediation activities within cyberspace itself. Many of the entities examined in this context were involved in agitating to have certain types of conduct or content in cyberspace deemed 'dangerous', 'inappropriate', 'illegal', and/or 'harmful'. However, my concern here is not with the claims making activities associated with defining and labeling such content and/or conduct. Rather, my main purpose is to describe how these agents and authorities took up and interpreted the problem of securing-child-safety-in-cyberspace and the strategies of direct intervention or indirect intermediation they developed in an effort to address it. A cursory examination shows that a broad array of networks aimed at the securitization of children has formed, and that a plethora of intermediary and intervention activities have evolved. A full blown investigation of all of these networks is neither intended nor attempted here. Rather, the investigation here will proceed by way of series of cases studies which aim to exemplify some of the more distinct characteristics of securitization as a strategic mode of intervention and intermediation. The chapter raises and responds to a number of important questions including: who are the interveners and intermediaries? What is the nature of their authority? What kinds of practices do they engage in at the level of intermediation and intervention? What kinds of consequences attach to their intervention activities?

The archive of data drawn upon for the purposes of investigating these questions came from a variety of sources. The primary orientation in terms of the

analysis of these documents was factual. My aim was to provide a broad descriptive account of the actors involved, and the sorts of intervention and intermediation activities they engaged in within contexts of operation. To be more precise, my aims were fourfold: to shed light and lend insight into the way that those involved in intervention and/or intermediation have tended to interpret the issue; to explore the self-conception of such actors in terms of their perception of their roles and responsibilities in relation to the issue; to provide a clear account of the approaches that have been adopted by them in terms of the means and measures being employed; and finally, to explore the implications associated with such employment.

In establishing the relevant background understanding for this stage of the investigation, I examined a number of strategic policy documents produced by the government of Canada, including the definitive 1997 strategy entitled 'Connecting Canadians' and sundry associated documents produced by Information Highway Advisory Council. In terms of substantive documents directly related to state intervention, I relied on presentations and reports from police agencies and private and third sector organizations and notes from two Conferences I attended which were hosted by the Society for the Policing of Cyberspace. Additionally, I have relied on information gathered from websites at the Home Office in the United Kingdom, the Virtual Crime Task Force, and several third sector organizations. With respect to private sector intermediation I relied on a number of position and policy papers released by the Canadian

Consortium of Information Service Providers, as well as contracts and terms of use stipulated by specific service providers.

Finally, in relation to third sector organizations, the primary data were gathered online – making reference to both existing web site information and the Internet 'Way-Back-Machine' to compile information that had been deleted from host sites or providers. A specific caveat or qualification ought to be attached to the data derived from these sources. Namely, my approach to their analysis was not predicated on any assumptions about the factual accuracy of the claims they make with respect to the representation of their activities. Indeed, any such supposition would require a much more methodical and detailed research design than the one offered here. Rather, my main aim in the analysis was to describe how these organizations represent themselves and the self-understandings that such representations reflect about their perception of the nature of the problem and what they believe it is necessary to do to address it.

***

We have seen that initial worries about bringing the power of criminal sanction to bear in cyberspace raised the more general question of whether cyberspace could be policed at all (pp. 8-12). An associated line of interrogation asked: who could conceivably police cyberspace and under what authority? And still in this connection, a third line of discussion began to develop about the kinds of arrangements and infrastructure which would be necessary to support police actions in cyberspace, the sorts of strategies and tactics which might be brought to bear, and ultimately, the potential efficacy of such undertakings. I have

suggested that these worries were, at least in part, attributable to a larger set of anxieties associated with the management of technological change and that the strategies adopted to address them need to be understood in terms of the modes of managing risk and security characteristic of neo-liberal societies. This emphasis on risk management has had a clear impact on approaches to policing as an institution and as a set of practices. I have alluded to the processes of transformation underway in policing, and described some of the key changes underway with respect to the security sector earlier in this investigation. The purpose of this discussion was to foreground the fact that security provision is the dominant mode of risk management in neo-liberal democracies, but also to acknowledge the extent to which a diversity of state and non-state agents are now involved in a variety of activities which were formerly constituted as the exclusive purview of the public police (Ericson and Haggerty 1997). Classical conceptions of policing, focused on the idea of law enforcement, are not descriptive of risk societies. Furthermore, the state-centric conception of policing is passé, as significant bodies of empirical research have shown extensive private sector involvement in tasks formerly thought to be the exclusive purview of the public police, and perhaps more importantly, as such research suggested both bleeding and blurring between notions 'public' and 'private' to the extent that the meaning of either term was increasingly difficult to determine[142] (Murphy 2005; Hermer *et al.* 2005; Shearing and Stenning 1981).

---

[142] This is not simply a case of slippery signification, but rather a reflection of a concrete changes in the use of spaces: not only were a broader spectrum of players involved in a diversity of policing activities, the places and spaces they policed were neither unambiguously public nor unequivocally private.

Nowhere is this diversity of involvement more pronounced than in relation to direct intervention approaches to securitizing the Internet. Over the last number of years we have seen the formation of a vast variety of agencies and organizations devoted to stopping child predators and child pornographers. Some of these agencies and organizations work in a stand-alone way, while others have invested time and effort building alliances and networks for risk communication, education, prevention and harm reduction. While direct intervention may consist in a variety of different activities, the organizations I consider here are treated under a common rubric in so far as they are not oriented toward technological fixes but rather are oriented to acting directly in cyberspace. The majority of such organizations involve people acting with the aim of altering the character and kinds of behavior that are going on in cyberspace, enlisting the help of law enforcement when they deem it necessary to do so, and in some special cases, acting upon and instituting their own sense of justice.

Given the aforementioned transformations in the nature of security and policing, the analysis developed in this chapter can be read as an attempt to respond to Hermer *et al.*' s (2005) observation that there is 'a paucity of studies on the networks with inter-related practices and outcomes associated with the provision of security'. These authors not only lament the extent to which the role of state police is typically privileged in criminological analyses, but also opine that it is 'too often implied that paid non-state policing agencies operate with a greater degree of disconnection from state police than is often the case' (Hermer *et al.*

2005). As a corrective to this state centric focus, Hermer *et al.* have argued that a model of security based on nodes and networks ought to be embraced in order to reflect the fact that security today is organized in a wide variety of ways including: agencies banding together to pool resources to sponsor policing initiatives (business improvement districts), states employing private security and private investigators, states contracting with local communities, states creating legislative environments conducive to non-state or semi-sate policing, and insurance companies making private security a condition of insurance (Hermer *et al.* 2005:47).

In fact, the theme of public-private partnerships in the assembly of security and its subsequent governance has become an almost emblematic feature at meetings of those involved in the provision of cyber-security, and it functions as a recurring motif in trade and technical papers devoted to addressing the state of security in cyberspace. In the context of the Internet, however, it is necessary to stress the extent to which third sector organizations play a role not only as a 'node' in the overall network of security governance, but as an instigator or prime mover in terms of new initiatives.[143] This reality points to a significant shortcoming in Wall's (1999) model for conceptualizing levels and processes of 'policing' in relation to cyberspace. To be more precise, Wall has offered a multi-layered conception of the structure of policing arrangements. According to his conception, police functions online bear a resemblance to structures offline. Wall thus distinguishes between five levels: the user level, the level of service

[143] Indeed, as we have already seen that the organization SafeSurf played a key role in the PICS initiative – as did Net Nanny in the development of the censorware approach.

providers, content hosts, corporations and corporate security organizations, and state funded non-public organizations. The role of third sector organizations receives only passing mention in this model, and it is largely related to intervention activities at the level of the user. One of the purposes of this chapter will be to show that third sector organizations play a much larger role and to make space for a clearer conception of their impact within a larger theoretical framework.

6.1 Tactical Approaches to Intervention and Intermediation

My argument to this point has been that securitization may be defined as a strategic mode of action which aims to address, reduce, minimize or manage risk by altering its conditions of possibility.[144] It follows from this definition that those modes of direct intervention that have law enforcement as their primary aim will not be examined here. This exclusion is not intended to suggest that enforcing the law does not alter a given risks' 'conditions of possibility'. Indeed, to the extent that it results in successful prosecutions and convictions – law enforcement may both effectively diminish the pool of available perpetrators and create widespread deterrence effects. Since a pool of available and motivated

[144] This processual conception is more specific than Johnston and Shearing's adumbration that security lies in that domain of intentional actions 'whose purpose is to provide guarantees of safety to subjects, both in the present and in the future' (2003:5). However, like them, I would acknowledge that strategies of securitization are subject to a variety of empirical vicissitudes that make their success the subject of some contingency. In other words, while these strategies may aim at producing guarantees, the intended effects are not always realized: practices and 'programs will fall short of giving people an effective assurance of peace' (2003:6).

perpetrators is one condition of possibility of risk to child safety online, law enforcement can have a clear impact.

However, in so far as the term 'strategy' is here understood as a long term plan to achieve a specific goal through the employment of designated means, what identifies securitization as a strategic mode of address is that it aims to achieve its goal through preventative means. It is not a matter of bringing offenders to justice: by then it is too late. It is a matter of preventing an offense in the first place. Some of the more obvious ways that the security needs of children have been operationalized in relation to this strategy in terms of intervention and intermediation include: seek-and-report patrols aimed at the identification and preemptive removal of objectionable material and/or questionable behavior, 'questionable material' report hotlines and networked reporting systems, and third sector regulative efforts and private sector self-regulative activities. We have also seen the formation of a number of novel securitization strategies that operate at the level of intermediation and direct intervention, including: tactics aimed at the disruption of the social networks which support pedophilic and predatory activity, infiltrate and expose campaigns, and diversion and detainment operations. In what follows, I describe several such initiatives and discuss the role they play in the overall network of intervention and intermediation.

6.2 Disrupt and Deter: Operation Pin

At the international level of efforts to protect children by state agencies, one of the most intriguing strategies aimed at addressing child pornography and

pedophiles has been Operation Pin. Operation Pin marks a decisive shift in police rationality with respect to child safety in cyberspace. To be more precise, what we see with the implementation of Operation Pin is a shift away from a mode of intervention which aims at the detection and identification of those who trade in child pornography with the longer term aim of building a chain of evidence sufficient to support prosecution. Instead, Operation Pin is a tactical form of intervention aimed at a fundamental disruption of trust within pedophile networks and embodies a strategy of *punitive deterrence.*[145] According to the official account of its origin – Operation Pin was the brainchild of detective Sharon Girling, a child pornography specialist in the West Midlands in the United Kingdom who has become a leading figure in the fight against child pornography. Girling was also involved in the earlier 'Indecent Images' initiative which used composite analysis to identify children in pornographic photos or video by focusing on a variety of background features in photographs and films in order to try to locate the site at which the photos or video were taken.[146] This program has

---

[145] My use of this nomination is intended to connote that we have a special strategy of deterrence at work here. First, deterrence here is neither general nor specific. To be considered a specific form of deterrence presumes that the person to whom it is applied had been legally established to have committed a crime. To be general deterrence it would have to be indirect – that is – not being applied to the person under consideration at all, but serving as an example to them. That it is punitive in form is beyond question. In so far as falsely advises the person that they are under investigation and it is hard to how imagine how any person so advised would not suffer some psychological torment.

[146] This highly discrete content analysis has been adopted by a variety of police agencies around the world. In a notable case related to Canadian law enforcement the Sex Crimes Unit of the Toronto Police Service found images of the same girl on the hard drives of many of the child pornography offenders, they used Photoshop technology to digitally remove her from some of the images and then released them to the public in 2004, asking for assistance in identifying the locations depicted could be identified The possibilities associated with utilizing such an approach had already been identified by Paul Gillespie in testimony before the Parliamentary Standing Committee on Justice and Human Rights in October of 2003.

proved highly successful and has been adopted by many forces around the globe.

There is, however, a 'back story' behind the development of the 'disrupt and deter' strategy embodied in Operation Pin. Namely, the shift in strategy can be interpreted as an attempt to avoid further exacerbating the backlog in the English courts created by Operation Ore, a previous sting in which police netted the addresses of over 7000 suspected child pornographers. The backlog from *Operation Ore* is so severe in fact, that the Midlands police department announced publicly that it would devote itself almost exclusively to preparing to prosecute the cases.[147] According to the Midlands police on this account, Operation Ore revealed that, contrary to popular wisdom with respect to pedophiles being 'risk aversive', many were not adverse to taking risks by stepping outside of their own tightly closed network. Indeed, it revealed that many pedophiles were not worried about using their credit cards to get access to illicit materials.

Originally envisaged as a stop gap measure in the United Kingdom alone, Operation Pin eventually became the pet project of the Virtual Global Task Force – an international police networking initiative that conjoins the RCMP, FBI, Interpol, Australian High Tech Crime Squad and the United Kingdom National Crime squad. The *modus operandi* of the project consists in the development of a number of what are called 'honey pot' websites. These websites are advertised and promoted on the Internet as sites which contain child pornography. However,

---

http://cmte.parl.gc.ca/Content/HOC/committee/372/just/evidence/ev1092114/justev67-e.htm#Int-711850

[147] The backlog continues to plague the English courts to this day.

should someone actually use their credit card to gain access to such materials, what they discover instead is that they have reached a law enforcement site whereupon they receive notification that they have violated the law and that their personal information has been recorded and may be passed on to local authorities. It also advises them that they have a problem, and that they should seek help immediately and it provides resources for them to seek out help. The purpose of building such 'honey pots' is not to create a chain of evidence sufficient to prosecute offenders. It is rather, first and foremost, a crime reduction initiative which aims at deterrence by creating a generalized sense of fear and uncertainty amongst pedophiles about the safety of their activities. The aim is to make 'the Internet an increasingly hostile and dangerous place for those seeking images of child abuse'. One of the self-identified secondary objectives, beyond shocking potential pedophiles and those who covet child pornography with the reality that they have been detected, is to create a pervasive sense of fear and mistrust in the wider pedophile and predator community. It is believed that creating such fear may disrupt what might otherwise be a rather 'seamless and relatively unproblematic' progression to deeper and deeper levels of integration within the community of pedophiles. To the extent that the design of Operation Pin is predicated upon research that depicts such networks in terms of a differential association account of their behavior[148], Operation Pin was devised as a means to prevent peer socialization, inhibit a sense of solidarity and destabilize support networks which would normalize a sexual interest in

[148] See, for example, the comments of Dr Rachel O'Connell, research director at the Cyberspace Research Centre at the University of Central Lancashire, as reported by the BBC (December 18, 2003).

children.[149] Operation Pin therefore tries to 'discourage those who facilitate the supply of images of child abuse online and undermine the confidence of those who hope to use the Internet anonymously when searching for sexual gratification by viewing images of child sexual abuse'.

A final objective of Operation Pin is to make it clear to pedophiles that the same rules regarding obscenity and pornography apply online as they do offline. The efficacy of Pin is also partly a function of its ability to keep the websites it produces relatively fresh – given communication between networks of pedophiles on the web. Since prosecution is not the primary aim, one of the distinct advantages of Operation Pin is that it does not have to engage directly with the issue of whether the alias identity given by the person online actually corresponds to who the person is in real life. Indeed, the problem of authenticating identity, which has long plagued more traditional approaches based on a law enforcement model, is by-passed completely.

6.3 Project Amnesty: Confess and Assess

A second interventionist approach consistent with securitization that also reflects a fairly significant shift in orientation is the 'Hard Drive Amnesty' program currently being contemplated by the United Kingdom home office. The program, which has not had yet had the green light in terms of implementation, is nonetheless very important and significant for our present purposes because it

[149] Operation Pin is predicated on the deeper set of casual assumptions when it comes to sexual crimes against children. Namely, that access to images online can fuel the fantasy life of pedophiles to the extent that it may ultimately prompt them to act out their fantasies in the real world. It should be noted that there is a great deal of contestation and debate in the literature – as well as the courts – over whether this is the case.

marks the appearance of new nomination in the struggle to secure children in cyberspace: 'proto-pedophiles'. Donald Findlater was the key mover in the formation of this initiative. Findlater is deputy director of the child protection charity 'Lucy Faithful Foundation'. The main idea of the program is to 'help nip child abuse in the bud'.[150] The underlying idea is that there is a high risk group of people who are what the initiative describes as 'proto-pedophiles'.[151] For these people, as their exposure to child pornography increases, so too does the likelihood that they will offend against children. Mr. Findlater's idea is that the problem must be stopped before it gets to the stage that the person is actually thinking about offending.[152] He argues that the current system of prosecution is not efficacious; the consequences in terms of vilification by the media are such that even people who know they have a problem will avoid coming forward for fear or reprisal, loss of reputation, job and family.

The operational scheme, which initially seems similar to gun amnesty, is actually one which goes much further beyond it. The idea is that for people who have been looking at child porn online, there will be evidence of such activity on their hard drives. Individuals who think they may have a problem or feel that they are starting to develop a problem may opt to remove their hard drives and bring them into local authorities. The drives are not examined but simply erased. The program then requires the individual to undergo psychiatric assessment in order to make a determination as to whether they are at risk of becoming pedophiles. Those found to be at risk would have to agree to undergo treatment or face

[150] http://www.ccpas.co.uk/Press%20releases/27%20Jan%202005.htm
[151] http://www.ccpas.co.uk/Press%20releases/27%20Jan%202005.htm
[152] http://news.bbc.co.uk/2/hi/uk_news/magazine/3254382.stm

prosecution. In the event that a proto-pedophile successfully completes treatment he is then given a warning regarding further contact with such materials. The Amnesty project has come under considerable fire from a variety of critics. One of the central issues in question concerns how effective existing approaches to treatment are; there continues to be considerable disagreement within the psychological and psychiatric community around this issue.

6.4 Bait and Expose: Virtual Vigilantism and Perverted Justice

Perverted.Justice.com is an online 'anti-pedophile' group that began operations in April of 2002. The group is composed of four full-time staff and approximately 75 volunteers at any given time. Their F.A.Q.[153] indicates that in terms of the backgrounds of the volunteer component approximately 50% are victims of sexual abuse. The group works to expose what it describes as 'wannabe pedophiles', which it characterizes as 'an epidemic problem'. These are predators that lurk in chat rooms looking for underage girls and boys. The self-proclaimed aim of the group according to its website is to deliver 'offenders' to law enforcement whenever possible[154], but this turns out to be a recent commitment that the organization made after considerable complaints and public pressure. The modus operandi of the group is to have volunteers pose as underage minors (typically between 10 and 15 years of age) in chat rooms. When they receive a message from another occupant of the group they engage

[153] The frequently asked questions page on the website.
[154] 'Concerned citizens from all walks of life who saw this problem got together and formed civilian watchdog group 'Perverted Justice', a website dedicated to finding and exposing those users in regional chat rooms with predatory tendencies towards children'. http://www.perverted-justice.com/guide/

in conversations. The full text interaction of these chats is logged both by the Yahoo server system and by a remote server, creating a chain of evidence. When the conversations turn toward sex and sexuality, the volunteers play along – often resulting in an extensive transcript that can span days or even weeks – and goes into graphic detail. Whereas state police would run the risk of entrapment, the volunteers at Perverted Justice face no such limitations, freeing them to inhabit their roles and furnish them with the kind of dramatic flourish necessary to create a rich evidentiary reservoir. The extent to which the volunteers engaged in role playing their underage is quite striking. A close analysis of these transcripts shows that the volunteers often play the roles of damaged and/or broken children with great dramatic realism and effect.

The term 'Perverted Justice' refers to the fact that the group acts directly against the predator/perpetrator, by posting transcripts of the chats online as well as pictures of the alleged predators. The intended purpose of these posts is to draw public attention and humiliation to the culprits. Frequently the group will go beyond such online measures, however. In a special section of their discussion board they ask members of the Perverted Justice community at large to track down information about the alleged predators including home and work addresses, telephone numbers, license plates and other information. This information is subsequently used to contact friends, employers, relatives and criminal justice authorities to notify them of the conduct of the alleged predator. One of the most interesting things about Perverted Justice is their open acknowledgement that it is not always clear that the activities that they are

exposing are illegal, and that it depends on the law of the territory or state where the person is residing.

In addition to this core activity, Perverted Justice also does training for police. The focus of this training is on teaching police officers how to pose as under age children and on how to conduct a successful investigation. Recently, the group was contracted to train state police in Arkansas. It would fitting to identify this group as 'moral entrepreneurs' – for they are surely engaged in moralizing behavior. However, they are not really targeting their efforts at the State, or at law enforcement, as is often typical of the period of agitation described in the social problems framework (Blumer 1971). Indeed, their intent is not to embarrass law enforcement at all but act directly upon what they see as the problem. The site, however, does contain many long laments about the sorry state of the justice system and a clear and abiding theme is that it is too lax and not effective.

In fact, prior to 2004, Perverted Justice had problems winning the support of law enforcement. Through a great deal of outreach, particularly by building contacts on the right and amongst religious groups in the United States, they claim to have won some recognition. Perverted Justice now reports that it maintains ties with many police forces across the United States and boasts 65 convictions as a result of their operations in cyberspace. It also claims to have been involved in the successful resolution of two child abduction rescues.

The Perverted Justice website prominently displays a link entitled 'Info for police' – inside of which one learns that Perverted Justice operates on what they

call an 'Information First' policy. The way that this procedure works is that once they establish contact with a suspected predator and build a record of evidence to support their allegation, they then reach out to the law enforcement agency located in the area where the predator is believed to reside. The law enforcement agency is provided with all of the details of the investigation – including transcripts of the chats, photographs, and phone information. The law enforcement agency then has the prerogative to decide whether it wants to follow up on the case. In the event that it does decide to do so, Perverted Justice suspends any further action in relation to the case for an unspecified period of time. If it is felt that the law enforcement agency is not acting with the appropriate alacrity, or if the law enforcement agency declines to pursue the case, Perverted Justice then follows its own protocol of posting the chat transcripts, with pictures and phone information, and may even enlist the help of its broader community to track down the offender and notify everyone connected to him about his actions. The notification process may include telephone calls to next of kin, faxes to the work place and, in some cases, a local Perverted Justice volunteer may print up signs with the picture of the alleged perpetrator on them and post them around the community in which he resides.

Perverted Justice also offers an accused predator what they call the 'right of reply'. In this case, someone who is accused may respond to the accusations by offering an explanation. If the person owns up and agrees to get help, Perverted Justice may decide not to post their profile. However, there is no indication on the site that they have ever elected to forego posting an alleged

perpetrator's profile. Finally, it is noteworthy that a number of agencies have grown up in opposition the activities of 'Perverted.Justice.Com', in particular Corrupted.Justice.Com. This group is devoted to opposing the tactics used by Perverted Justice and to exposing Perverted Justice as a fraudulent organization.

6.5 Search and Destroy: Ethical Hackers against Pedophilia

A second organization devoted to virtual vigilantism is the group known as Ethical Hackers against Child Pornography (EHAP). The group formed in July 1997 by a number of hackers who identify themselves only in terms of their online handles, avatars or pseudonyms. For a short time the group maintained an affiliation with another hacker group (consisting of Se7en and Modify) but eventually separated into its own entity. The specific details associated with its processes of formation are difficult to garner and gather together, for reasons that shall be discussed shortly.

According to archived records, EHAP's purpose is 'to combat the production and dissemination of child pornography and to assist law enforcement in locating the perpetrators'. The group makes a variety of claims about itself and the activities in which it engages that are of interest in so far as they reveal something about the self-understanding of those who are involved. However, to the extent that many of these claims are not validated – an attitude of circumspection toward their claims seems judicious. As a major motivation for its formation, the group cites a massive growth in the availability and distribution of child pornography on the Internet and it portrays itself as 'a last ditch effort to

help control the overwhelming problems that can readily seen on the Internet involved with pedophilia'. In this context the group constructs child pornography and pedophilia online as an epidemic problem and one which requires the most extreme measures to address.

EHAP maintained a public façade and hosted a website which featured key details associated with their aims and objectives until 2003. After that point in time, the group decided to remove any and all traces of its mandate and identity from current Internet servers and went underground, citing significant fear of retaliation in reaction to their work. EHAP, which is purported to still be operative in the United States, constructs its role as one of a 'go-between'. It works to protect the identity of those who find child pornography and to protect their anonymity while working closely with law enforcement. For public purposes, EHAP denies that it engages in vigilante activity and has issued several statements to this effect:

> A common question is how we go about our task when informed about a site. Most of our methods and techniques are classified; however, we like to dispel the notion that we merely hack a site and remove whatever is there, and get out. We instead like to work closely with the law, and use national, and in some cases, international contacts to help us put away these perpetrators for good.

However, this denial does not jive with many of the claims made by the group elsewhere. For example, in several interviews with founding members in Wired Magazine and Mondo 2600, the group members relate stories about having hacked into and brought down a significant child pornography sites in Russia –

and of having infiltrated a number of traders' computers and deleted their hard drives.

6.6 Patrol to Report: Adult Porn, Cyber-Angels and the Morally Militant

The rise of direct action citizen-police networks represents one of the most interesting phenomena with respect to intervention and intermediation actions in cyberspace. While the rise of such groups online bears some parallels with the development of such groups in community contexts, a number of features unique to cyberspace distinguish these groups from their 'real-world' counterparts. Citizen patrols can be understood as 'relatively autonomous groups of citizens who engage themselves on a voluntary basis in patrolling a limited geographic area with the broad aim of enhancing security' (Leech 2002). In this section, I review some of the literature associated with citizen patrols and subsequently present an analysis of several online groups whose activities bear some similarities to these offline activities: Cyber-Angels, TeenAngels, Adult Sites Against Child Pornography, and Antichildporn.org. While all four groups engage in functions which conform to the classical conception of policing, their aims, objectives and tactics are distinct. Indeed, they proceed from quite differing conceptions of the character of the dangers at hand, and these differing definitions are reflected in what they feel it is necessary to do to try to make the Internet a safe and secure place. The first two organizations adopt what can be characterized as seek, find and report functions. They set up teams who patrol together and have a reporting protocol that involves notifying ISPs of offensive

content and ensuring it is removed. The other organizations are far more active in orientation. They see their role as more than simply identifying sites where illegal material is being shown and notifying the ISP of the site, or in cases where deemed necessary, notifying local law enforcement. The third group is one which maintains a reporting function and does follow up investigation for the purposes of determining if the complaint is *bona fide*. The final group is one which wants to make sure that the judicial apparatus is brought to bear. Hence, they take a more aggressive role with information service providers, insisting that it is not a matter of merely blocking the site but of contacting law enforcement and working toward the collection of a chain of evidence that will be sufficient to support charges and ideally, a conviction. This reflects their conviction that sites that are simply deleted will result in the offending parties simply going elsewhere.[155]

The trend toward citizen involvement in policing in this context has been interpreted as 'a moment of civic participation' and 'the proliferation of citizen patrols may reflect a transition in the character of citizenship' (Leech 2002). At the same time, however, the patrolling activities of these organizations ought not to be immediately be cloaked with the mantle of civic virtue (Leech 2002). Indeed, the formation of such groups is sometimes a reflection of reaction to the inadequacy of state security provisions. Such efforts are sometimes rooted in intolerance (Leech 2002). The considerations which may motivate people to form a patrol group are diverse. Understanding these motivations is key to arriving at an understanding of their actions. The rise of citizen patrol groups online parallels

---

[155] A similar line of argument arose when MSN announced it would close its chat groups to those who were not subscribers.

the development of such groups in community contexts and raises some similar sets questions. However, there are several features that make cyber-patrol groups particularly problematic in contrast to more conventional citizen patrol groups. First, the issue of territory is nebulous. Indeed, while citizen patrol groups operating in physical space may be motivated by the 'conviction that greater security will be achieved for their communities by taking the issue into their own hands' (Leech 2002) it is difficult to identify a similar locale with respect to cyberspace groups. Leech notes that the scope of a neighborhood patrols' 'activities may vary tremendously' (2002). However, one does not find typically find any reference to geographical location amongst cyber-patrol groups. Hence, it is often the case that these groups define the whole Internet as the community they patrol. Second, while citizen patrols in communities and neighborhoods are often coordinated by police, this is not the case in cyberspace.

Cyber-Angels is exemplary in this respect. They describe themselves as 'a cyber-neighborhood watch' that operates 'worldwide in cyberspace'. Cyber-Angels was founded by Curtis Sliwa, founder and president of the Guardian Angels. Formed in 1995, Cyber-Angels claims to be the largest 'online safety, education and help' organization. The organization began by addressing 'cyber stalking' in Internet Relay Chat Rooms (IRCs), but later decided to extend its activity to include 'child pornography patrols' aimed at finding and reporting child pornography online. Approximately two years later it began to offer workshops for online safety issues. In 1998 the organization decided to focus more directly on the World Wide Web and specifically on parents and law enforcement: 'Parents

needed help in supervising their children's web-surfing. Law enforcement needed support and knowledgeable assistance in tracking cyber-predators and understanding online crimes. There needed to be as large a contingent heralding the good things about the Internet, as warning about the risks.'[156] This included a number of outreach activities online.

Cyber-Angels constructs it mission explicitly as one aimed at protecting the innocent online, with secondary goals of helping law enforcement and educating users about safety and technology.[157] The basic activities of the organization could be broadly categorized under the headings risk communication and risk education, but there is also a process of moral education that goes on here. The group does not confine itself to a specific set of risks, but rather addresses a wide variety of issues including: 'inappropriate display of adult materials, kiddy porn, hacker sites'. A range of individuals are involved in the program, but recruiting emphasis is placed on people with backgrounds in law enforcement and the legal professional, as well as Internet technology specialists, translators, teachers, librarians, and mental health professionals. Cyber-Angels has been officially recognized[158] by law enforcement agencies for its work in locating online crimes and criminal content, such as child pornography, predators and stalkers. It has also assisted law enforcement agents at the level of training, providing instruction on cybercrime investigations, tracking online pedophile material, hacking and/or cyber-terrorism, and cyber-

---

[156] http://www.cyberangels.org/volunteer/index.html
[157] http://www.cyberangels.org/volunteer/index.html
[158] A number of police forces in the United States have sent the organization letters of commendation.

fraud. Furthermore it boasts that it has frequently provided information to law enforcement agencies for the purposes of arrest.

In addition to organizations like Cyber-Angels run and staffed by adults, we have also seen the rise of a number of peer-to-peer organizations which patrol cyberspace and educate children. The most prominent of these is Teen-Angels, a youth oriented version of Cyber-Angels.[159] The organization recruits young volunteers who 'armed with Internet savvy and a little common sense' go into cyberspace in order to protect their peers online. They teach web surfers 'how they can avoid criminals who prey on children by using e-mail, online chat rooms and even instant messages to contact them'.[160] The other target population of the organization is parents. The stated aim of the group is not to petrify parents but to help them not to be afraid. 'TeenAngels' was an initiative of the New York lawyer Parry Aftab, who specializes in security and privacy law. The main idea of TeenAngels is that the kids may not be willing to listen to adults, and also that kids know more about the realities of cyberspace than do adults. The organization gathers information from police services about patterns of victimization and legislation that may apply to different geographical areas. The main idea is that these kids provide good role models. Its primary function in this regard is to disseminate information to schools and through the website which is complemented by the groups' educational video production. The organization also has the support of the FBI in the United States. In addition to seek and find reporting functions and educational functions, TeenAngels also

---

[159] http://www.wiredkids.org/teenangels/squads/index.htm
[160] http://www.eschoolnews.com/news/showstory.cfm?ArticleID=2989

designs web pages on safety for kids, and issues regular bulletins to its members containing articles about recent events in relation to child safety.

Beyond mere patrol and report activities, several agencies actually engage in independent investigative functions and report the results of their investigation to police authorities after they have determined or decided upon the validity of the complaint. One group involved in such direct investigation is the 'Association of Sites Advocating Child Protection' (ASACP). The group, which formed in 1996, was formerly known as 'Adult Sites against Child Pornography', but changed its name sometime after 2003 for reasons that are not indicated. ASACP was started by Alec Helmy, president and publisher of XBiz[161], to help the professional adult industry disassociate itself from child pornography.[162] Once a corporation, now a registered not-for-profit, ASACP relies on three classes of sponsorship for its survival: Platinum, Title and Corporate. Some of the sponsors involved in the Platinum classes are called affiliates or Internet payment companies - companies that facilitate the use of credit cards in the processes of making transactions to pay for access adult Internet entertainment sites. Others are content providers.

Although the efforts of ASACP might be seen simply as an attempt by the adult entertainment industry to defray public concern about pornography by taking some responsibility for self-regulation, the rational and motivational background are more complicated. Indeed, one of the key concerns of the group

---

[161] XBIZ is the adult entertainment industry's 'first large-format trade publication, with a focus on balanced business news, market trends, growth sectors, and international news in the online, offline, mobile and ancillary sectors (http://www.xbizworld.com/)
[162] http://www.xbizworld.com/

is not so much to protect children, as to protect 'legitimate' and respectable consumers of adult pornography from the possibility that they might be exposed to child pornography through one of their subscriptions, and thereby be implicated in some sort of illegality. As a matter of fact, the group stipulates that it formed partly in response to 'industry' fears of about losing customers – who in turn had indicated an unwillingness to renew subscriptions or continue with services because they feared they might inadvertently download or view child pornography.

The group claims that it is specially positioned to respond to complaints because it has an insider's knowledge of the industry. It also positions itself as a 'conduit' agency that acts as an intermediary between the police and surfers who come across child pornography but would be reluctant to report their discover directly to police or who would not otherwise report possible child pornography and sexual abuse to police. The group provides a variety of resources for those who operate, or want to operate, adult content sites and want to do so in a way that is not harmful for children. [163]

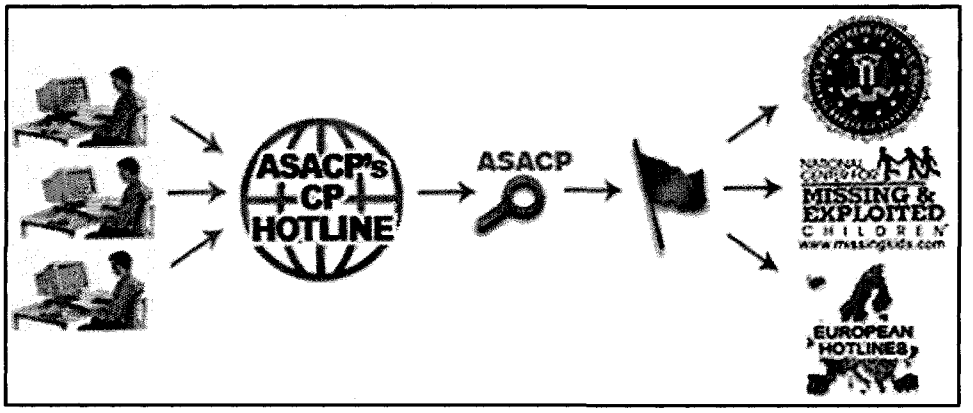

Figure 9: ASACP Communications/Investigations Model

[163] http://www.asacp.org/statistics.php

ASACP runs an online reporting hotline. One of the noteworthy things about this reporting system is its specificity. To be more precise, it has a clear focus on commercial sites. Hence, those who have come across content they feel is child pornography are advised not to complain to them if it comes from Usenet Newsgroups, Chat boards, Instant Messaging, BBS Message boards, Web communities (Yahoo, MSN, AOL and Lycos), or Peer-to-Peer Sources (Kazaa and Morpheus), rather they are referred by hotlink to the U.S. National Centre for Missing and Exploited Children.

	October 2006	Since 2003
Raw Reports Received by Hotline	4,818	176,901
Average Reports Per Day	155	151
Red Flag Reports Forwarded	171	4,101

Table 2: Total Reports to ASCAP

Adult Sites Against Child Pornography attempts to get out in front of false positives by stipulating as clearly as possible what kinds of content are legal and should not be complained about. Hence it indicates, for the purposes of heading off complaints and educating consumers, that the following are not illegal in the U.S: 'sites with text describing child pornography, child modeling sites, animations, drawings and cartoons'.[164] Interestingly enough, there is no reference made to the possibility that such content may prove illegal in other countries, nor are standards in other countries referred to as points of reference.

[164] http://www.asacp.org/

The organization also stresses that child nudity is not necessarily child pornography and refers potential complainants to more information in order to make the differentiation.

The processes involved in following up on complaints are not clear on the ASACP site, nor were subsequent request for clarification answered. It appears that the organization retains the right of final determination in so far deciding whether to reports submitted to the hot line are followed up internally or whether they are submitted by them to the authorities. Those who do make a report to the ASACP site receive a verification notice upon submission, and a subsequent follow up response by email indicating whether their complaint was turned over to the authorities.

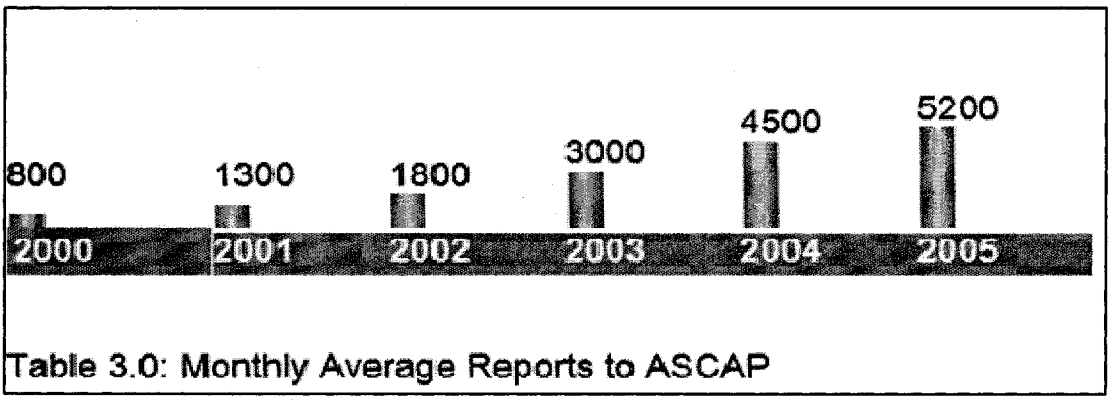

Table 3.0: Monthly Average Reports to ASCAP

Since its inception in 2003, ASACP indicates that it has fielded over 175,000 reports. Of those received, however, it has forwarded less than 3%. This is a fairly significant rate of false positives and raises a larger set of questions about the criteria involved in investigating complaints and making judgments as to their validity. ASACP does not provide a clear account of the whole investigative approach they follow, nor do they offer an account of how they go

about ascertaining whether a given 'model' was of age in the photography or video under investigation.

ASACP has also created a free for use label to assist children and adults in surfing the Internet more safety. The organization claims that this label will help filtering systems in navigating away from sites that might be offensive or have deleterious effects on children. However, the meta-tagging protocols necessary to enable such navigation are not present on the site – directing the Webmaster to a dead link.[165]

Finally, with further respect to self-regulation,[166]ASACP also operates what they describe as an 'Approved Member program' for adult sites. Approved Member sites are required to comply with a Code of Ethics. This code of ethics does not confine itself to addressing websites alone but also addresses search engines and directories, billing companies, TGP's, Hosting Companies and Adult Dating Sites. The content of the code of ethics is fairly limited to the extent that it could easily be interpreted as an industry attempt to meet the minimum requirements of due diligence in relation to the appearance of child pornography. In this regard, a list of prohibited meta-tags is provided – but is hardly one which would be considered exhaustive.[167] The Code of Ethics further stipulates that sites need to make a 'good faith' effort to comply with the current standard of recordkeeping of the US Government. They are also encouraged to post 'in a prominent position' notices through their sites that 'all models were 18 or older at

---

[165] http://www.asacp.org/page.php?content=webmaster. Retrieved July 27, 2007.
[166] http://www.asacp.org/RTA.php
[167] Indeed, looking at the lingo of purveyors and traders, a much larger list of terms is required (2001).

the time of depiction'. In the cases where a model is 18 but looks younger, the statement should be reiterated. Furthermore, sites which direct traffic to the host site should be periodically examined for their use of unacceptable terms.[168] Members of ASACP are encouraged to do business with companies that comply with the ASACP Code of Ethics. And finally, they may display an Approved ASACP Member insignia on site as a testimonial that the site does not contain nor condone child pornography.

One of the recurring complaints of ASACP relates to their inability to gain the cooperation of law enforcement. Although the activities of ASACP have been acknowledged by both the U.S. Customs Agency and the FBI, the organization complains of a lack of communication. These agencies are reluctant to work with such organizations. According to the adult entertainment industry lobby group, the 'Free Speech Coalition', this refusal to cooperate is due to the fact that:

> The government does not want us in business, period...They don't care if we have cleaner sites. They use the child-porn issue as the linchpin for bringing down the adult industry. If we don't police ourselves, they'll do it for us.

It is difficult to know how much credibility to attach to this complaint. However, further research into the issue would be of value in helping to conceptualize the kinds of barriers that may arise in terms of the formation of alliances between different organizations and agencies devoted to protecting the security of children in cyberspace and how they may impact on the overall effort.

---

[168] Including Adolescent, Child, Child porn, Child sex, Children, Kiddie, Kiddie porn, Kiddie sex, Lolitas, Minor, Minors, Pedoland, Pedophile, Pedophilia, Pre-teen, Pre-teen porn, Pre-teen sex, Teen13-17 and Underaged.

A number of non-profit organizations have been established to raise public awareness about the issue of Internet child pornography and to act as political lobby groups. These groups include *Wired Safety* and *Safeguarding Our Children*. Another web based group, www.pedowatch.com, offers a free, downloadable tool called Digger Engine, along with detailed techniques to trace Internet Relay Chat users and Usenet posts. Among such groups the ACPO (antichildporn.org) is the most militant in its approach. A non-profit group formed in 2001, it explicitly seeks out and investigates the exploitation of children on the Internet with a secondary purpose of public education. ACPO's self-identified goals include investigating child porn and assisting law enforcement investigations. In direct response to the hype created by the media about child pornography, its defined purpose is to put pressure on public authorities to act on the problem – and to form networks and alliances with other like-minded organizations and agencies. The key plank of ACPO is the reporting service it runs. This provides the basic information for the investigations that follow. The aim of these investigations is to build a case for police. While ACPO supports freedom of speech, they make it clear that they see citizen involvement in the process of bringing community standards to bear on cyberspace as crucial, and hence, their role is as a proactive responsible citizen. Aside from investigation, much of the work of ACPO as an organization has been devoted to networking, building alliances and supporting nascent organizations devoted to the same cause in their bid to get up and operational. In this context they have helped and

cooperated with other organizations like Safe-Guarding Our Children – United Mothers[169] and Anti-Kinder-Porno.[170]

6.7 Embedded Information Service Providers in the Network of Intermediaries

The role of ISPs in mediating Internet content remains controversial. One of the most common themes, repeated time and time again by police agencies is that they require the cooperation of the private sector in order to successfully address the problems of child pornography and predatory behavior. ISPs in

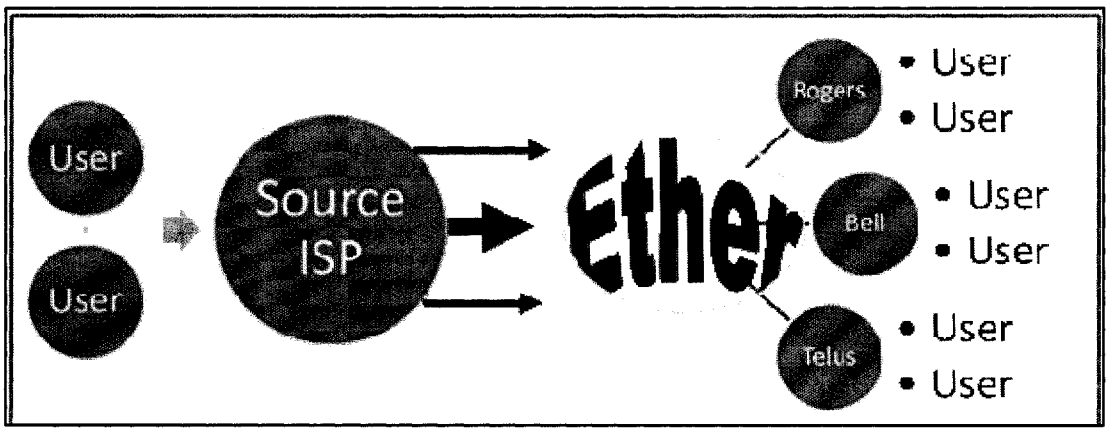

Figure 10: Network Control Approaches

Canada, however, construct the question of their cooperation with police as a difficult one. Indeed, the constant refrain from ISPs is that they are businesses and have contracts with their clients and must obey the 'Terms of Service' set out in these contracts. Thus, they play the role of good corporate citizens in so far as the public stance of Bell-Sympatico and Rogers has been that they want to see a stop to the harmful conduct and content online, but at the same time, they must acknowledge and respect the privacy rights of their clients. It is hence not

[169] http://www.soc-um.org/
[170] http://www.antikinderporno.ch/

feasible to simply invite the police in and get their assistance in terms of investigation. Notwithstanding these objections, it is clear that these service providers do have a variety of mechanisms in place for monitoring user's habits and practices and that they do intervene actively where misuse or wrong doing is suspected (Winseck 2002). Security work in these contexts is often outsourced to third parties. One of the largest such outsourcing companies is Convergis, with offices across Canada and the U.S., extending to Pakistan. These agents have the authority to recommend fraud investigations, notify police about unauthorized access, and conduct investigations. The function of these personnel is to monitor security and safeguard the integrity of the system. They use password generators – supplying random passwords to clients and respond to queries about firewalls.

Recently, we have begun to see some changes in posture in relation to the role of ISPs. It used to be the case that they were considered common carriers and thus not liable for the content they carried. However, that may be changing. For example, British Telecom is now working with the Internet Watch Foundation (IWF) to prevent their customers from accessing child porn. The system is called 'clean feed' and works by having IWF provide a list of sites to be blacklisted. The state of Pennsylvania recently passed legislation that allows the Attorney General to apply for court orders which will direct ISPs in the state to block access to websites which contain illegal content. The case of Australia provides another example. The Australian broadcast authority has established codes that govern the availability of inappropriate material on the Internet. The

codes are address to ISPs and require them to make safety tools and information available on the home sites. The other change requires that such service providers restrict the transmission of context classified as X and place restrictions on users who try to access restricted or mature adult rated content.

6.8 Cyber-Security as Parapolice: A New Class of Regulatory Agents

Long before the advent of the Internet, the use of computers to store and transmit valuable information had prompted the growth of a formalized body of knowledge devoted to 'computer security' as well as the development of specialized occupations in computer security. With the rise of networking, however, and more particularly, with the connection of local area networks to the Internet, new forms of occupational specialization have arisen that conjoin technical knowledge with policing and surveillance functions: paradigmatic in this respect are the systems operator and the network security specialist. The language of information and network security is overwhelmingly one of prevention and risk management.[171] Indeed, one of the primary functions of these specialists is to serve as risk communicators. Moreover, the typical security planning model is built around a risk management framework wherein hazards are conceptualized and operationalized in terms of system strengths and vulnerabilities, and action plans are formulated accordingly. It needs to be acknowledged that these organizational roles have formed and are now

[171] For example, security specialists work with others to envision and develop a high-technology-crime prevention plan. Another risk management strategy involves the circulation of surveys to 'identify threats, areas of vulnerability and risk' (Kovacich *et al.* 2000).

embedded across government, private and third sector organizations and that a wide range of intermediary and interventionist authority may be allocated to these positions.[172] In so far as the duties, authorities and range of responsibilities exercised in relation to these positions vary, some examples may be of service.

System operators at the university level are involved in a variety of surveillance functions including monitoring bandwidth and storage, responding to and investigating complaint about improper usage, and developing terms of reference for users. They also engage in some forms of moral regulation. For example, they may create blacklists of UseNet groups that will not be downloaded to the local server and therefore cannot be accessed by subscribers. In the United States, they may also be called upon to examine employee uses or audit and forensically assess hard drives. An excellent example of how these activities may bear upon the safety of children in cyberspace occurred in the case of a Carleton student who was involved in a white supremacist group and sent email messages out to children some elementary schools in Ottawa. The incident prompted an internal investigation. A second case occurred in Canada where a routine audit of bandwidth usage by an information security specialist at DND revealed that a ranking member of the Department was involved in collecting and distributing child pornography using the government T1 system. This case, which garnered much media attention, raised a variety of questions

[172] I have not undertaken an extensive investigation of the roles and responsibilities associated with these occupations. However, I did consult several information security specialist texts as well as visiting the Association of Security specialist's website.

about how issues of security were being approached within government.[173] It is noteworthy that the Communications Security Establishment has played an ongoing role in securing governmental systems at the level of intrusion and threat protection measures, but that the establishment of general security maintenance, auditing, and reporting procedures is left under the internal organizational rubric of each department.

The rise of these new classes of regulatory agents warrants consideration for a number of reasons. First, they are contexts in which threats are envisioned and strategies for securitization are operationalized and implemented. Second, in the context where these information security specialists are in the employ of private companies, IPSs or the like, there is no requirement for disclosure to public authorities in the event of breaches. This means that the orientation toward loss prevention or protecting the good reputation of the company may prevail over other concerns associated with bringing the State police into action. Third, and related, this means that the actions of many who work in the computer security sector are seldom transparent or subject to any processes of oversight or public accountability. Much of the work involved in computer security is imperceptible; the consequences of decisions made in terms of security protocols remain arcane to users of networks. And, more to the point, almost all of the alterations made at the level of security operate below the threshold of perception. Fourth, the functions born by these individuals bear similarities to police or private security functions more generally. For example, like private

---

[173] DND revealed that a ranking member of the Department had been accessing and downloading child pornography.

security guards, they are empowered to eject individuals from particular cyberspaces if that individual is deemed to have violated the terms of use according to their interpretation of them (not the interpretation of a judiciary or law enforcement officer). Fifth, these individuals often have the power to subject you and whatever is contained in your logs and storage allocation to search and seizure. Sixth, these parapolice also exercise powers that extend beyond those typically exercised by the public police. For example, system operators enjoy a considerable amount of latitude in determining what is 'unacceptable' and 'acceptable' content and or conduct according to the Terms of Service agreements. They make daily judgments in this respect and frequently these decisions are without a process of appeal.

6.9 Summation

The foregoing analysis showed that a broad array of networks aimed at the securitization of children has formed, and that a plethora of intermediary and intervention activities have evolved. It describes several classes of interveners and intermediaries involved in a variety of securitization functions ranging from public education and outreach, to monitoring and surveillance, to patrol and reporting to direct intervention. The authority associated with the activities of these agents varied from that which was officially sanctioned to purely voluntary and relatively free-floating. The exploration showed that several of the activities underway in terms of direct intervention are worthy of additional attention and investigation. This is particularly true in the relation to the tactic of punitive

deterrence, which would seem to represent a departure from the basic commitment of law enforcement to observing the law. The appearance of the idea of a proto-pedophile as the basis for justifying intervention is also noteworthy and worthy of further investigation. Finally, the activities of the organization Perverted Justice mark a significant departure from the basic logic of securitization and ought to be examined more closely.

Chapter Seven:

Modes of Securitization in Combination

7.0 Security as an Assemblage in the Context of Emplacement

The foregoing analyses have suggested that it is important to distinguish between the problem solving processes underway in the contexts of design, operation, and emplacement. We should acknowledge that the approaches adopted to address the problem may reflect not only differing interpretations of its essential nature and/or extent, but also differing convictions as to the corrigibility of the problem in general and differing perceptions of the agents who share responsibility for addressing it.

The analyses also showed that while securitization is the dominant strategic response to the child-safety-in-cyberspace problematic, the tactical embodiments of this strategy take distinct forms in different domains. To be more precise, the analyses thus far traced the logics of securitization in design contexts to tactics of embedding, and the analyses of the logics of securitization in operational contexts identified the twin tactics of preventative intervention and intermediation. If we accept that the combined effect of action in these two contexts is to prefigure and mediate conduct and content in cyberspace in significant ways, it remains to be seen how the child-security-in-cyberspace problematic is interpreted in contexts of emplacement and how these interpretations motivate certain forms of action while proscribing others.

This chapter describes the historical processes of securitization that involved attempts to render manageable generalized risks to children which are

created by the insecurities of cyberspace. These involved a variety of tactics aimed at instilling precautionary behavior (preventative habits and using practices aimed at minimizing risk) and surveillance systems aimed at specific deterrence. In contexts of emplacement, these tactics are intended to engender accountability, social responsibility, and an individualized awareness of, and orientation toward, self-protection. The analysis will show that the 'securing-child-safety-in-cyberspace' problematic is subject to a very broad interpretation in contexts of emplacement, to the extent that it exhibits indications of both stretching and traveling.[174] Indeed, in these contexts we find an approach to risk management that verges on becoming totalizing in so far as it involves comprehensive tactics of responsibilization (Hacking 2002; Dean 1999). Three modes of responsibilization are evident in this context: direct, by-proxy, and client-contract.[175] In the first case, tactics of responsibilization take aim at children themselves, understood as end-users. In the second case, they take aim at the parents and other in *loco-parentis* authorities. Finally, in the third case, they take aim at the client or consumer as a party to a contract.

In the first section I describe some of the ways that media discourses, as well as materials produced by state and non-state agencies, position parents as

---

[174] The description of these phenomena is taken from the discussion of the definition of terrorism discussed by Weinberg *et al.* (2004): 'In the process of arguing over the meaning or interpretation of a given situation, 'disputants engage in a number of processes that actually make it more ambiguous; in particular, they subject it to 'border' and 'membership' problems, as well as 'stretching' and 'traveling' problems' (Weinberg *et al.* 2004).

[175] While Dean suggests an interesting descriptive terminology to describe the effect of processes of responsibilization ('technologies of agency' and 'technologies of citizenship') – I have not chosen to draw upon his conception here in so far as it seems to confuse rather than clarify the relationship between the actors and the technologies (Dean 1999: 147).

ultimately responsible for the welfare of their children in cyberspace, as well as aim to arm and equip them with the tools and knowledge necessary to take on such responsibility. I argue, following Hacking, that not only is risk the dominant structure of interpretation in this context, but that we can understand the ensuing processes of responsibilization as reflecting an expansion in the risk portfolio associated with parenting.[176]

7.1 Theoretical and Conceptual Preliminaries

Responsibilization can be understood in the most basic way as a process of assigning to parties the power and authority to govern and manage the risks related to their biographies and also of attributing to them, or imbuing within them, a sense of responsibility for the *contingency of their successes*[177] in undertaking to assume such responsibility. Responsibilization thus involves promoting self-reliance and abandoning a welfare mentality wherein community members accept curtailment of certain freedoms in contracting community law enforcement to ensure their safety and protection (Sullivan 2001). Individuals are instead encouraged to take measures of their choice that provide for the safety, security and protection of themselves and their family members (Sullivan 2001). Strategies aimed at the responsibilization of the user emphasize the individual's

---

[176] A broad way to highlight this expansion would be to pose the question: 'When the state steps back from using whatever mechanisms and measures would allow it to directly provide for the protection of children in cyberspace (like instituting a comprehensive regime of censorship, or subjecting Internet traffic to selective screening), who inherits the responsibility for regulation, and whose risk portfolio does it become part of?'

[177] The italicized language associated with this caveat is mine. However, I think that Hacking alludes to this point, if not making it outright, when he suggests that the logic of the individualization of risk leads to a form of blaming the victim (2002).

role as a contributor to the maintenance and proper ordering of virtual spaces. The power and freedom to order and control one's virtual environment is depicted as requiring the user to exercise diligence and prudence, to be respectful, to have 'moral competencies', and overall, to have an awareness and a responsibility to the greater Internet community. Hence, in referring to an individual's use of code-based regulation, Spinello asserts 'users must make well-informed and conscientious choices about software, and they must also make every effort to implement and utilize the software in the most responsible way possible' (2002:61). Approaches to securitization through responsibilization may aim at changing the 'end-user environment' in three ways: by altering para-technical relations, by changing the content of cyberspace itself (through filtering or blocking), or by any combination of these.

The data I have drawn upon for the purposes of the analyses come from an assortment of sources. A variety of literatures have been produced by state agencies, private and third sector organizations aimed at helping children to take responsibility for their safety in cyberspace and aimed at helping parents to take responsibility for the safety of their children. The data for this chapter includes manuals from the RCMP, the FBI, and from SchoolNet. I have also examined a great deal of the material from the Live Wires site – with a particular focus on the 'Missing' kit – which was distributed to elementary schools across Canada. I also looked at debates that arose in two parenting forums on the Internet. I examined a number of strategic policy documents produced by the government of Canada. I also relied on presentations and reports from Canadian police agencies and

private organizations. Finally, I have relied on information gathered from websites at the Home Office in the United Kingdom, the Virtual Crime Task Force, and several third sector organizations.[178]

These data are sufficient to afford a broad understanding of the way that the problem of child-safety in cyberspace is presented to parents and children in the context of the classroom and household. Since it would be difficult to confirm that these literatures are broadly representative of the vast array of materials and approaches addressing the issue in these contexts, I have treated these materials in a manner that is consistent with their specificity as case studies. It is important to note that the findings arrived at in this chapter are not presented as – or imagined to be – representative of all representations; nor do I contend that the tactic of responsibilization in relation to securing children and empowering adults is the exclusive or only approach involved in such processes of governance in the household.

Although the argumentative groundwork to support the analysis in this chapter was laid out earlier, it may be useful to re-examine the main points to underscore the import of contemporary neo-liberal modes of governance. Whereas welfarist approaches witnessed an expansion of the state, neo-liberalism involves a general withdrawal from socialized forms of intervention and an emphasis on minimalist modes of governance that work at a distance (Dean 1999). The governing mentalities of neo-liberalism, and the ontological assumptions that underlie it, produce a tension between autonomy and dependence where 'conducting the conduct' of children is of concern. The child

[178] See Appendix A for a table of data and primary sources.

and/or childhood are problematic for liberalism in so far as it is a predicated on a commitment to the conception of individuals within society as autonomous and self-determining. This cannot be directly conferred upon children as a population, however, without contradiction. Yet, at the same time, it has withdrawn from the very forms of intervention which would allow it to manage the needs associated with their dependency directly. It therefore finds itself in the paradoxical position of being reliant on a civil society and the private and third sector to provide such protections.

Understanding the processes associated with the emplacement of cyberspace in households and the construction of security needs in relation to this process therefore also means examining prevailing understandings of childhood and parenting and understanding the way that childhood as a state, and parenting as a process, are constructed and managed within liberal and neo-liberal discourses. The development of structures to govern the security of children in cyberspace must thus be understood as structurally conditioned by this tension within neo-liberalism. To be more precise, this tension gives rise to a unique set of risk management problematics which are seen both in the rise of third sector powers devoted to addressing them, and in the distinct set of tactics which emerge to provide for the safety of children through governance at a distance.

7.2 The Role of the Media, State, Private and Third Sectors in Responsibilization

The analysis in Chapter Three described some of the claims and claims makers involved in the processes by which the safety of children in cyberspace emerged as a problematic, and alluded to the fact that parents were often represented as ultimately 'responsible' for addressing this problem. In introducing this section I want to expand upon this line of analysis by offering additional findings yielded by the media analysis described in Chapter Three, but reserved for discussion here because they were deemed more germane. To be clear, I have already indicated that parents are the subject of, and subject to, a constant stream of exhortations, edicts and entreaties in newspaper narratives directing them to assume responsibility for the safety of their children in cyberspace. Now I will describe the role that private and third sector organizations have played in this overall process. I begin by describing narratives about the family and subsequently attempt to excavate something of the moral subtext associated with these narratives. In this context, three issues associated with questions of trust are singled out for closer analysis. The first is whether cyberspace is actually a place that can be trusted at all. The second is whether the judgment of children can be trusted in relation to materials and or activities that might prove harmful and/or dangerous. Third, there is a more general question as to whether children are ultimately 'trustworthy' at all.

With particular regard to the process of responsibilization where the safety of children in cyberspace is concerned, we find that both state and non-state agencies repeatedly refer to, locate, and narrate the family as the most salient

context appropriate and proper for attending to children's security needs in so far as these are part of the custodial functions of parenthood. The analysis also suggests that flows of responsibility are involved, wherein the bailiwick and authority of institutions and individuals can be conceptualized using the concept of risk portfolios. Messaging by the state locates the responsibility for managing these risks shifts in the family as an institution, in the parents as caregivers, and in the school as a site of computer education.[179]

While some studies have tended to emphasize that moral forms of governance are on the decline, other scholars contend that morality has not disappeared but is increasingly integrated within the calculative logic underlying risk as a modality of governance (Ericson and Doyle 2003). The analysis of the responsibilization of households and parents confirms the latter assertion. Indeed, there are a plethora of parties involved in making moralizing claims in relation to the roles and responsibilities of households and parents. Corporations, law enforcement, educators, government officials, media, vigilante groups, community organizations and other social actors have a vested interest in the moralization of conduct.[180] The general character of this moralization is seen in

---

[179] It could be argued that through these and other processes of responsibilization aimed at family structures and parenting, the state has renegotiated the role it may formerly have played in negotiating the tension between autonomy and dependence. However, such a line of argument would require a much more sustained investigation and analysis.

[180] For instance, community health centers in Ottawa receive money for cyber bullying projects, to the extent that they have to succeed in problematizing that behavior they have also been able to secure more funding. A more recent example of moralization facilitating social action is the collaboration between Microsoft and international law enforcement to create a child exploitation tracking system. The prelude to this partnership was a sustained public relations campaign staged by the Toronto Child Exploitation Unit aimed at generating public awareness and concern about the problem.

the set of assertions about the kinds of steps that 'reasonable parents' would want to take in relation to their children. Such parents either already have taken the time to get to know the risks that their children face in cyberspace or will make the effort to do so upon learning of their ignorance.

The moral flavor of these discourses melds with risk rationalities in so far as the emphasis is placed upon the idea that choices carry with them the consequences and the associated implication of parental supervisory culpability for child victimization. This idea of culpability is particularly pronounced in media narratives around victimization incidents in which we see that events redefined in such a way as to responsibilize parents of victims (Hacking 2002). We see corollaries of this logic in cases where hackers who attack are successful; the cause is re-defined as one not explicable solely in terms of an adroit predator, but also in terms of a parent or guardian who is irresponsible in so far as s/he is inattentive to security concerns. Just as those who did not buy insurance have brought their misfortune on themselves if they are robbed, so too are those parents who failed to purchase filtering software or to establish means and mechanisms of surveillance and control deemed culpable in the event that the sexual purity of their children is violated.

One of the more *sub rosa* modes of responsibilization through moralization arises is in relation to consequentialist discourses which focus on worst case scenarios. Sunstein argues that this kind of emphasis – affected by

the availability heuristic[181] - may lead to probability neglect (2004). In this case, the severity of the consequences associated with the possibility of victimization are amplified and magnified to the extent that an 'at any cost' imperative necessary to avoid such victimization becomes paramount. The very idea of allowing for any possibility of such victimization is held up as indicative of parental negligence, and thus the role of parents in relation to cyberspace is redefined such that they must not only know at all times where their children are, but that they must know what they are doing. The effect of such discourses is that the security needs of children are re-defined in such a way that the children themselves cannot be trusted to know them, and as a consequence, they cannot be trusted at all. Indeed, amongst parents who accept this darker construction of risk, spying on your children in cyberspace is part of behaving like a responsible parent.

A recurring message in many narratives, from newspaper reports to manuals produced by the police to help pages provided by third sector groups, is that while cyberspace is not trustworthy, the risk cannot be avoided. You cannot simply refuse to allow your child Internet access because this would be detrimental to the child; facility on the Internet and savvy in cyberspace is overwhelmingly presented as an integral to a child's overall development. Hence, 'pulling the plug' in order to protect your child is not an option. This rationality might be linked to, and informed by, a larger understanding of child-rearing as something which aims at optimizing the inner potential of the child. In this

[181] Or a cognitive bias in which people imagine that simply because an event or instance of some behavior can easily be brought to mind it must therefore be a frequent occurrence.

context, Giddens has talked about the self-reflexive character of biographical construction and the phenomenon of inflationary expectations where achievement and distinction are concerned (2002). The general identification with one's progeny promotes the emphasis on maximizing your child's potential, as do the many media narratives around family which emphasize the primacy of consanguinity. We can also make sense of the need for children to become cyber-literate from a Foucauldian bio-political perspective – according to which nurturing new generations with marketable skills and abilities is crucial to the strength of the state (Foucault 1991). There is, nonetheless, a definite tension within many of these narratives between, on the one hand, an understanding that counter-poses cyberspace and safety, implying that there is no safety to be had in cyberspace, and, on the other, narratives which relate that the only real way to secure the safety of children is parental supervision.

With respect to the trustworthiness of children it is noteworthy that securitization through responsibilization is not only a matter of parents addressing and acting upon the conditions of possibility for risk. Rather, children need to be responsibilized because the mere presence of children in cyberspace is one condition of possibility for their safety being at risk. As we will see shortly, such responsibilization must be delivered in a manner that is much akin to target hardening.[182] To be more precise, children must be made to recognize and

---

[182] Target hardening is a crime prevention strategy that functions through opportunity reduction. The animating idea is that the commission of the crime is made as difficult as possible by making the physical conditions resistance to its commission. The purpose of such efforts is both to increase resistance if someone does attempt to commit a crime, as well signaling to the general pool of available offenders that the hardened site is not a good target.

accept their vulnerability and to adopt certain normative imperatives or edicts in relation to it. Such imperatives appear in the form of 'advisories' provided to parents which present a variety of strategies parents may want to consider. Key in all cases is that children must be educated to understand that both their safety and their innocence are at risk and must be protected by them. One of the chief quandaries associated with protecting the innocence of children through such education is what I would call the *inoculation dilemma*. In an effort to safeguard the safety and sexual innocence of children, the parent may opt to tell them that there are people out there who will harm them, and want to do things with them that are wrong. However, the very act of telling the child this information may result in a loss of some innocence. However, if this loss is acknowledged, it is typically constructed as manageable and its cost is portrayed as worth its benefit.

7.3 Securing Innocence: End-User Oriented Approaches

In order to explore the process whereby children are constituted as responsible for their own safety and security, I make use of the notion of responsibilization. As discussed earlier, Foucault was interested in the historical processes underlying the formation of procedures by which the subject is led 'to observe itself, to analyze itself, to decipher itself, and to recognize itself as a domain of possible knowledge' (Florence 1994:316). Technologies of the self can encompass forms of self-narration, self care, and self-understanding. These are understood to contribute both to the forms in which our subjectivity is constituted

and experienced, as well as to the forms in which we govern our thought and conduct.[183]

Approaches to securitization through responsibilization may aim at changing the habits and dispositions of children as 'end-users' or at changing the 'end-user environment' by altering para-technical relations. On cursory inspection, end-user oriented security discourses are highly diverse and they appear in a wide variety of formats, reflecting a great plurality of perspectives and a range of objectives. For the purposes of this analysis, end-user oriented discourses have been classified by strategy. In some cases, these strategies consist in brokering a contract between the child and the parents and/or teacher; in other cases, these strategies attempt to achieve greater security by instilling in child users a set of attitudes and beliefs about cyberspace itself, and to use those beliefs as a basis to establish appropriate behavioral dispositions and cognitive habits. Other end-user oriented security strategies not only individualize risk and responsibilize individual security, but enlist individuals in the broader project of securing cyberspace more generally.

One widely advocated way of approaching and constructing a solution to the problem of security with children is through the vehicle of a contract. This suggestion, with sample copies of contracts, is found in the safety resources pages of many websites, and is recommended by many police agencies and

---

[183] Foucault argued that the domain of sexuality had become a privileged site of such self-relations and was concerned to ask why sexual conduct became an object of moral solicitude (1991): 'Foucault looked for the forms and modalities of the relation to self by which the individual constitutes and recognizes himself qua subject' (Davidson 1990:243).

schools. The content of such contracts is variable, but three themes appear to be recurrent.[184] The first and most prominent theme is that of 'discomfort'. In contract after contract, discomfort is constructed as the 'threshold' which requires reporting upon and reporting about. The subjective character of this term is conserved in these contracts, rather than subject to some sort of additional attempts at clarification. Such a strategy aims to recognize that different children have different levels of sensitivity, but also that any more specificity may have the effect of excluding from the range of reports discomfort instances that parents would have preferred to know about. Any discomfort should be reported – just in case its source is in untoward behavior or inappropriate content. Most contracts stipulate that the child will inform the parents of such occurrences immediately.[185] A second theme in parent -child contracts is the prospect of meeting someone offline that you first met online. Contracts differ on this count – a few indicate that such meetings are just not a good practice under any circumstances, because it is a slippery slope, while the majority suggest that such meetings must be cleared by parents in advance, and set out other stipulations for the meeting including, for example, that it must be in a public place, and that it must be during the daytime. Some suggest that such a meeting should take place only under the accompaniment and supervision of a parent. A third and final issue that is

---

[184] Before discussing these, however, I think it is important to consider the socialization effects associated with having children enter into contracts. After all, the breach of such contracts is not likely to result in legal liability – rather the contract is a symbolic artifact of an agreement. It is also interesting to note that none of the contracts stipulate penalties for violation. Presumably this is because it is understood that this matter should be left up to the discretion of the parents.

[185] That the 'source' of the discomfort need not be specified and, in almost all cases, is not specified – suggests that the precautionary principle is at work here.

noteworthy in the contexts of contracts is the question of follow up on the contract. Some websites discuss the possibility of penalties for violation, including suspension of access to the Internet, while others indicate that penalties should be negotiated with children so that it is made clear that violations will have consequences.

A second set of tactics utilized in order to responsibilize children for their own safety in cyberspace are those which aim at instilling in them a set of attitudes and beliefs about the dangers in cyberspace and thus imbuing them with behavioral dispositions and cognitive convictions that will support their safety. One example of such an approach, developed by the Media Awareness Network, is a computerized role playing game in which children are brought into a fantasy world wherein they play the roles, in seriatim, of four different children who have been lured to the studio of a child pornographer. The role playing part of the activity for the children begins with their imagining having been forced to pose for the photographer and having him become abusive when they would not pose in ways that pleased him. Children are invited at this point to make diary entries in a journal which would reflect the child's point of view. In other words: 'What would it be like to be held hostage in that place? What would it feel like to be held captive in that place? What would it feel like to have someone trying to take pictures of you that made you uncomfortable?' The exercise is intended to get children to think about, learn through empathy and eventually come to understand how children gradually come under the control of predatory pornographers. In another episode of the same game, children role play a child

who is trying to flee from the predator/pornographer's house. This game is fast paced and adrenal, requiring the children to make split second decisions about which way to go. It also features pop-up messages that indicate they are close to being 'caught' by their pursuer. It is hard to imagine that the role playing effect of being pursued by a child pornographer would not leave them full of adrenaline and fear. Another example taken from the 'Missing' literature invites children to critique a fictional website. The premise is:

> Websites do not just communicate facts. They also contain photographs that show how people feel. This information can be valuable to predators that are searching for children who are angry or unhappy. Look at the album pages (by clicking on the photos to the left) and examine the images carefully.[186]

One of the most powerful tools in inciting the formation of safe security practices involves teaching children to see themselves as regulatory agents. Key in this context is the existence of reporting structures beyond parents that provide avenues for children (and their parents) to commit to a sense of collective ownership over the content in cyberspace by acting in manners consistent with its care and protection. Children on AOL and KOL, for example, are advised that in the event that they do come across something that they feel is inappropriate or disturbing they should summon a community leader and report it immediately.[187] The idea that they can report such events is integral to giving them a sense of ownership over the space, but perhaps more importantly, it is integral to instilling

---

[186] The photographs are fairly, but not totally, ambiguous. They are meant to convey that Zack has communicated to a possible child predator that 1. His mother is away. 2. His mother and father do not get along. 3. He doesn't get on well with his friends and 4. His father is very busy.

[187] In fact, one of the key challenges that America Online has faced in this context is that they have not acted with enough alacrity for complainants.

within them the feeling that structures of action and accountability are in place. In some cases, children have been recruited into the activity of patrolling cyberspace and reporting on perceived violations of the law and offensive content.

7.4 At Home in the Classroom

It is worthwhile observing that while risk is individualized at the level of the household, the appearance of safe surfing and cyber-proofing courses at schools and sometimes in the mandatory curriculum represents some socialization of the risk. Like bicycle safety, the development of safe surfing habits requires instruction. A number of schools across Canada now offer courses on Internet safety, and programs on Internet safety are now offered by many parks and recreation departments. Indeed, officialdom has produced a variety of manuals, some aimed at children as the audience, others aimed at parents. In this section I describe and discuss three of the main themes that emerge out of the resources produced for use in classrooms in the Canadian context.

First, the overall orientation we find in these manuals is one which urges teachers to present the possible hazards and dangers in such a way that these are appropriately counter balanced by an emphasis on the benefits of the associated with developing a facility with the Internet. The stress in such manuals is to develop instructional units that will allow children to have exposure and experiences with the Internet that allow them to build their sense of confidence

about how to use the technology, and also to increase their sense that they know how to and can identify situations and circumstances which may present dangers or risks. In this context the constant emphasis is on the disclosure of personal information and the more general prohibition against meeting anyone in the real world who you first met online.

A second theme in the instructional manuals and handbooks developed for the use of teachers in the classroom emphasizes that the teacher themselves must become literate and Internet savvy, acquainting themselves with the safe spots where children can go as well as developing a broader awareness about the kinds of emerging threats that may present challenges to teaching Internet literacy in the classroom.

The final focus found throughout these manuals is the emphasis on the parents as the primary focus of decision making and judgment about proper Internet use. The curriculum indicates that teachers should encourage their students to set up a meeting with their parents to discuss the issues associated with securing themselves online, and in many contexts we find that the manuals suggest that the children be encouraged to take the initiative by teaching their parents about the Internet and surfing together.

7.5 Are You A Good Parent?

Thus far we have been talking about children and parents in a fairly unproblematic fashion. However, contrary to naturalistic conceptions of parenthood, childhood, and the family unit, these concepts and the social

formations they refer to are far from static. Discourses about parenting have a long history and it is necessary to emphasize that the idea of parenting is itself a recent invention, and especially that the idea of 'good' or 'proper' parenting has an even more recent history. Studies in the social sciences have traced the emergence of the idea of parenting to the construction of childhood (Ambert 1986). The practice of preaching to parents about how they ought to conduct the conduct of their children correspond in one way or another to a set of assumptions about the nature and needs of the child as a developing entity (Hunt 1999). Parenting, constructed as a skill and activity, is governed by a complex set of social and cultural expectations as well as legal norms. In the neo-liberal risk society, parenting is increasingly constructed as a matter of multitasking and managing a diverse portfolio of risks. In works which contend that the notion of childhood is a relatively recent invention, some argue that the category itself is in decline (Postman 1982). We have seen that the designation of the parent as a protector of the child stems from a certain set of assumptions about childhood as a time of innocence, and indeed, purity. In this context, Hacking describes the 'fear-for-our-children' as an 'overwhelming addition to the risk portfolio' and indicates that above all our fear is 'that our children will be defiled - subject to unspeakable filth' (Hacking 2003:44).

If we consider Marshall McLuhan's counter-instrumentalist insight about the way that technologies change human behavior and how people come to serve machines (1964), we would do well to ask whether and how parents have had to change their assumptions about what constitutes good parenting in order

to accommodate the exigencies associated with securing their children in cyberspace. Indeed, when we examine the processes that have accompanied the emplacement of the Internet into the household, we see that its presence has prompted several challenges to conventional wisdom about parenting and trust. The presence of the networked computer has been cited as a justification to alter the dynamics of spatial organization within the household. Indeed, according to the new normative imperative, the household must be re-organized to ensure the visibility of the computer: it must be placed in a common space, rather than in a bedroom, and it is not allowed to face the wall. Some manuals recommend that the screen should be visible at a distance. In this context, there has been an attempt to re-define computing as a family activity (a nomination which, not incidentally, belies the single operator character of the steering mechanisms).

Many thinkers have argued that one of the clear consequences of the development of risk rationalities is the development of a broad culture of fear, and that in this context the idea of hyper-vigilance may become a virtue and grow unchecked (Giddens 1990; Sunstein 2001). For the hyper-vigilant parent,[188] the balance between autonomy and dependency so central to the process of child rearing becomes problematic. Security can become the new fulcrum for creating a balance and boundary between the life of the adult and the life of the child. Reliance on the parent for protection is identified as a 'healthy' condition, but only in moderation. Indeed, in popular discourses, parenting is often constructed as a matter of navigating a variety of 'traps'. One such trap identified by the

[188] The term hyper-parenting was originally used to describe children whose lives are over-scheduled, but it is now being used to describe the obsessive orientation toward control exhibited by some parents.

psychological disciplines is over-protective parenting. Some argue that the effect of all of these precautionary and preventative discourses (imperatives toward maximum securitization) may be a kind of infantilization of children. The environs they have access to are so sterile and sanitized that they do not stimulate the development of children's interpretive and cognitive coping skills. Other experts argue that the effect of these discourses may be to bring children into a fragile and fearful sense of sexuality and their own vulnerability. Sunstein's critique of the precautionary principle is particularly *a propos* in this context in so far as he argues that by addressing some risks we always end up creating others (2001). What we see here is that parents are on the horns of a dilemma characterized by the risk of over-parenting on the one hand, and by the risk of under-parenting on the other. The dilemma is symptomatic of the tension between autonomy and dependence which is characteristic of contemporary neo-liberal societies and is thematized in a variety of ways throughout the discourses which responsibilize parents in relation to their children's use of the Internet.

It is tempting to interpret the issues at stake in the parental dilemma in terms of a typical trade-off model, in which children are required to cede some of their privacy for the sake of increasing their security. This formulation, however, belies the fact that there is a clear counter-current of resistance in evidence in reaction to such practices and that this counter-current too has structural roots. Indeed, definitions of security in the context of the household are subject to contestation and outright resistance. As I have indicated earlier, this is not the place to evaluate the overall efficacy of certain securitization approaches, but it is

important to acknowledge that some securitization strategies (particularly maximum surveillance and zero tolerance approaches) may inadvertently incite or stimulate unwanted behavior. Some of the literature developed for parents in regard to the use of monitoring software acknowledges that its use may have the unintended consequence of producing a secondary threat, namely that of deception. For children who want privacy, and believe they are entitled to it, Internet usage may become a matter of secrecy. This issue is noted because it is discussed by parents in the context of governing their security, and by children on many websites. Indeed, it is not uncommon to see threads with posts asking for help disabling such programs there. Again, this resistance might be traced back to the balancing act implicit in neo-liberal modes of governance.

7.6 Securitization as Assemblage: Parent as Bricoleur, Parent as Prosthesis

As has already been made clear in Chapter Six, parents who wish to 'be responsible' in terms of their child's safety in cyberspace may opt to rely on any number of technological or software solutions. These 'prostheses' may work to provide parents with more information[189], but the common consensus is that they are no substitute for parental involvement and thus, when employed, they should be used in combination with a more hands on approach. In this context, we have seen that parents may elect to deploy and/or employ any number of para-

[189] One particularly problematic conundrum in this context occurs when the filtering software fails to do its job and allows illicit content to be presented to the child. The surveillance software captures the illicit information and makes a record of its reception. What then? Can the parent determine or sort out whether this was an intentional act of defiance - or an accident? The question goes to the heart of 'trustworthiness'.

technical securitization strategies including relocating the home computer, instituting a contract, and establishing a diversity of auditing and reporting procedures with their children in order to govern terms of access, use and time periods, stipulating prohibited sites and banning potential chat and email correspondence. For the purposes of theoretical modeling, Haggerty and Ericson's (2000) notion of the surveillent assemblage provides a good vehicle for conceptualizing the array of strategies that are available and may be mobilized in the name of good parenting:

> For Haggerty and Ericson, what is notable about the emergent surveillant assemblage is that, driven by desires to bring component parts together into functional systems – variations on which take the form of control, governance, security and profit – an exponential increase in, and convergence of, surveillance technologies has ensued. They explain that surveillance capabilities are increasingly directed towards the human body as a distinctive composition of life forms and webs of information. These processes involve abstractions from, or data doubles of, organic hybrids, such that a protracted reliance develops on machines not only to register but record otherwise discrete observations (Hier 2003:413).

To be more precise, 'responsible parents' may avail themselves of a diverse assemblage of equipment that has emerged in relation to cyberspace safety and they may combine these with a variety of para-technical practices in order to create functional systems that work to govern the security of their children. We have seen in the previous chapter that the processes associated with governing security can be conceived in terms of a network constituted by key nodal points. We have also seen that a rich supply of resources is made available to parents by a variety of non-state and state agencies to govern the security of their children online. Parents may elect to employ any combination of

these and thus may customize their approach to a great degree. In so far as the variety of pieces available can be mixed and matched and adjusted to meet varying situations, parents take on the role of security bricoleur.

7.7 Responsibilizing Consumers

An interesting example of the use of responsibilization strategies in relation to consumers in the series of developments oriented to responsibilizing are consumers of pornography. As indicated earlier, ASACP is an organization devoted to making adult entertainment safe for adults to enjoy. To achieve this end ASACP has produced a series of pamphlets and educational releases aimed at educating consumers on 'Surfing Safely'. On initial analysis, the objectives associated with these guides appear to be protecting clientele. However, the construction of the issue of child endangerment by the ASACP suggests that there are moral questions at stake, and indeed, that those who enjoy Adult Entertainment on the Internet must also take responsibility for fighting the scourge of child pornography. In this respect, the website run by ASACP includes a bulletin board for testimonials that laud the work of the organization and especially emphasize that the problem of pedophilia and child pornography is everyone's business.

As well, there are several questions that arise in relation to attempts to responsibilize consumers. First, it is unclear whether and to what extent these programs are not at the same time countered by a significant portion of the pornographic industry which emphasizes and caters to a market for young, nubile boys and girls. The drive toward younger and younger models is demonstrated

by websites that aim at those with a taste for the 'barely legal', and indeed, there are a number of sites in this context which construct young men and women as particularly covetable sex objects precisely because they are innocent. Hence, the effect of such attempts to responsibilize customers may merely be posturing as opposed to arising out of a genuine desire to curb rather than cater to such tastes.

7.8 Summation

This chapter showed that the processes of securitization operating in contexts of emplacement were characterized by the common theme of responsibilization. It argued that responsibilization strategies function to redistribute the portfolio of risks, and that in the case of cyberspace, the major recipients of reassigned responsibilities have been parents. The investigation also showed that responsibilization strategies included attempts to foster the precautionary behavior and preventative habits in children by targeting teachers and creating curriculum modules. It also described some of the ways the family unit, and particularly parents were targeted as responsible for teaching their children to manage risk, and surveillance systems were created in the name of deterrence. Finally, each of these parties (teachers, parents, and children) involved here can be conceived as relevant social groups in so far as they are involved in conceptualizing the character of the problem under address, debating the nature of the techno-social environment they are dealing with and arriving at decisions about how to respond. Moreover, we can see that a high degree of

interpretive flexibility appears to characterize the relationship between these parties and can also point to significant contestation and debate in terms of the definition of security itself and the measures necessary to achieve it.

What is of additional interest here is that each of these parties (teachers, parents, children) can be conceived as relevant social groups in so far as they are involved in conceptualizing the character of the problem under address, debating the nature of the techno-social environment they are dealing with and arriving at decisions about how to respond. Moreover, we can see that a high degree of interpretive flexibility appears to characterize the relationship between these parties and can also point to significant contestation and debate in terms of the definition of security itself and the measures necessary to achieve it.

Chapter Eight: Conclusion

8.0 Introduction

The period immediately following the inception of the Internet can be broadly characterized in terms of a tension between extremes: tides of euphoria and jubilance on the one hand, and undercurrents of unease and uncertainty on the other. Hopes for the new technology were high, and a broad swell of public discourse celebrated the emergence of the Internet as a breakthrough of Promethean proportions. At the same time, however, there were abiding worries about the unruly character of cyberspace, and persistent reservations about whether it could be brought under the rule of law.

At the outset of this investigation it was suggested that this period in the history of the development of the Internet has not been well understood, and particularly that there has been a tendency to see and treat this period primarily as one in which the kinks associated with bringing the power of criminal law to bear on cyberspace were merely being worked out. I argued that this tendency ought to be resisted and fosters a false sense of the nature of our relationship with technology on the one hand, and disguises the role that human values play in influencing processes of technological change on the other. To be more precise, rather than focusing principally or primarily on adjustments to legal and regulatory infrastructures necessary to address the impact of the Internet, I argued that we ought to also look at how the technological system itself was subject to a series of modifications and adjustments. In this context I argued that the Internet has undergone a significant process of transformation in the name of

making it a safe space for children, and that the principal means by which this transformation occurred was securitization.

In what follows, I summarize the work and review the key findings. Subsequently, I identify some of the contributions the work makes to the broader theoretical and substantive literature. Next, I explore directions for further research and investigation. Finally, I look at some of the open questions in relation to the securitization of cyberspace. In closing, I offer some speculations about the current gradient and where it is likely to lead.

8.1 Summation of the work

The first phase of this thesis examined the conditions which gave rise to the emergence and formulation of the securing-child-safety-in-cyberspace problematic. My contention at the outset was that the emergence of this particular formulation as such was neither necessary, nor necessarily logical. Indeed, neither the emergence of this particular issue *per se*, nor its formulation in terms of the securing-child-safety-in-cyberspace problematic, were events that could be assumed as inevitable but were rather something that needed to be explained. With respect to the process of emergence, I contended that fears about the presence of child pornographers, child predators and pedophiles in cyberspace were, in and of themselves, not sufficient to account for the emergence of the prominence achieved by this particular worry. I argued that two structural characteristics associated with neo-liberal risk societies were also at work, enhancing the prominence of the issue and making it especially

susceptible to up-take. In the first case, I noted that neo-liberal governing mentalities are principally directed at autonomous self-determining individuals, that they wrestle with a tension between autonomy and dependence where children are at issue, and that this tension is particularly pronounced where questions of sexuality are involved. Second, I noted that neo-liberalism is marked by state withdrawal from most forms of direct intervention. This not only makes providing for the protection of children difficult, but produces a strain that engenders persistent feelings of anxiety both because the state finds itself without direct access to a population that it concedes is not wholly autonomous but whose welfare it nonetheless has a fiduciary duty to safeguard, and because these same rationalities designate children as a population vital to the future prosperity of the nation. The second condition identified was a general sense of apprehension about the pace and impact of technological development. To be more specific, I identified the second characteristic as a nagging and persistent sense of uncertainty and apprehension about modern trajectories of technological development that has increasingly come to characterize modern risk societies. I argued that this anxiety was exacerbated by risk logics which harp on and consistently highlight the vulnerability of children. Furthermore, I argued that an additional factor contributing to the broad scale society-wide process of problematization may have been a fusion between the first and second sorts of anxiety and the effects of this fusion would be witnessed in a redefinition of the nature and parameters of the problem, bringing a much

broader repertoire of threats under the rubric of risk and implicating a larger and more diverse population of possible agents in response.

In the next phase of the argument, I suggested that responses to the emergence of this generalized worry about the welfare of children in cyberspace could have taken any number of other forms or formulations.[190] I contended that while the combination of the aforementioned anxieties and media and market-place depictions of the threats to children in cyberspace created the conditions of possibility for the formation of a problematic, they did not explain why this particular problematic formed. In other words, they did not explain why the issue was framed and organized as one of securing-child-safety-in-cyberspace. In response to this interrogation, I argued that the footprint of the same two structural conditions identified earlier (risk logics and neo-liberal rationalities of rule) could be seen in the processes associated with this formulation and that they produced what could be described as a distinctly neo-liberal, risk inflected 'problematic' in so far as it: 1) reframed threats as risks manageable through prevention and precaution; 2) functioned as a call for action across a variety of institutional contexts; and 3) served as a call to arms to a variety of non-state actors. Put bluntly, the governing sensibilities of neo-liberalism and logics associated with risk management were accorded a decisive role in the formulation process. To be more precise, while the logic of risk 'organizes' children as a population 'at risk' by defining them as vulnerable, innocent and in need of protection, neo-liberal commitments rely on proxies and delegation to

---

[190] One extreme, though not necessarily inconceivable, response might have been a declaration of war on child predators, on pornographers and their ilk, for example.

protect this innocence and also to retain some sense of their agency. The trend toward delegation has been particularly pronounced in relation to the security of children, as witnessed in an extensive process of diversification and multi-lateralization in sources of security, the securitization of children has become 'everybody's business'. The structures of securitization that have developed in relation to the needs of children in cyberspace reflect these trends toward thinking in terms of security.

Once an account of the conditions which contributed to the formation of the child-safety-in-cyberspace problematic had been prepared, the second phase of the investigation could begin. This phase was intended to trace out and explore the consequences associated with the formulation of the problem as one of children's insecurity and to investigate the way that attempts to address this problem had evolved in three action contexts. At the most general level, the analysis showed that a wide array of actors and organizations (RSGs) were involved in the developing securitization strategies – and that this process involved the formation of new technologies, new nodes, new organizations[191] and new classes of regulatory agents. In other cases, this involved expanding objectives and sorting out jurisdictional issues. This was particularly evident in the case of schools, where a new curriculum and new programs were introduced to teach children how to surf safely. Furthermore, it showed that the objective of providing for the security of children was subject to a variety of different interpretations and the source of considerable conflict. In addition, interpretive

[191] It would, however, be misleading to overemphasize such novelty. Indeed, we have also seen that, in these same processes, existing agencies and organizations were brought in, though this involved some re-mandating and re-tasking resources.

diversity resulted in the development of a variety of different initiatives which employed different securitization strategies. The findings also showed that the conceptions of how security could ultimately be achieved, and of what was at stake, differed considerably. Finally, it showed that the responsibility for responding to the problem has been constructed in terms of the family and in terms of parental responsibility. The market, in this context, functioned not simply to generate demand for security products or to make different solutions available at the level of consumption, but also to vivify the threat and entrench the idea that this was a parental responsibility.

8.2 Discussion of Findings

Several findings in this study are of importance from the stand-point of the social construction of technology approach. First, it should be apparent that where complex systems like cyberspace are concerned, both problem formation and problem solving cannot be conceived in terms of any kind of linear model. This was noted early on in the investigation, but the findings of the work significantly substantiate it. Furthermore, the investigation of the conditions associated with the formation of a problematic benefited from the modified social problems model in two ways. First, it provided a broader macro level background and point of reference according to which the roles played by the media and market place, as well as larger neo-liberal risk logics, could be identified and better appreciated. This is important for thinkers working in the SCOT tradition since, as we have seen, they have been struggling to conceptualize the role of

exogenous factors. The investigation also suggested that SCOT researchers may want to give special consideration to the case of the Internet for two reasons. First, as a design environment it encompasses a wide spectrum of relevant social groups and allows for a high degree of interpretive flexibility both with respect to the nature of the problem and potential solution. Second and related, the investigation made it clear that closure is much more open and reversible where we are dealing with the evolution of the Internet.

A second area of findings of considerable importance relates to our thinking about, and understanding of, the logics of neo-liberalism and processes of securitization. To be more precise, the investigation showed that in the network of agencies and organizations involved in securitization processes concerned with intermediation and intervention, a decisive role was played by the third sector. This was clear both with respect to their processes of claims making in problematizing the safety of children more generally, but was especially pronounced in the development of securitization strategies and solutions. A great number of third sector organizations, agencies and groups have formed to contest the content and character of cyberspace. One of the obvious deductions that might be made in relation to this finding is that third sector organizations are in a much better position than are governments to respond to questions of harmful content and conduct in so far as they do not have to contend with the specter of state censorship. This theme certainly emerged in the analysis of SafeSurf. However, the moral dimension associated with the activities of these agencies and organizations should not be overlooked. Many of the organizations

discussed based their actions on moral positions and associated convictions about what cyberspace should be. We have seen that one of the prevailing precepts associated with neo-liberalism as an organizing governmentality is that it delegates the functions of moral education and regulation to sectors within civil society. However, the investigation showed quite clearly that in some cases this delegation can have unintended and arguably problematic consequences. This is particularly the case where the rise of virtual vigilantism is witnessed in response to cyber-predators.

A further set of findings in relation to logics of securitization which will prove of significant interest to those who study policing and are interested in the transmutation of police tactics and strategies pertains to the adoption of a number of prevention oriented interventions by state police in conjunction with third sector organizations. The most compelling example of this sort was Operation Pin, which represents a decisive step away from an emphasis on law enforcement and embodies instead an orientation toward diversion, disruption and punitive deterrence. A second, and related, finding bearing on police activity in cyberspace was the disclosure of the extent to which police are increasingly turning to third sector organizations for training in terms of policing conduct online. Perhaps most significant in this regard was the disclosure that the state police are being trained to pose as underage children in chat rooms by the volunteers at Perverted Justice. The ethical conduct of this organization is questionable, to be sure. But that police are seeking training from it must invariably have the effect of legitimating its activities.

8.3 Contributions of the Work

While this work makes valuable contributions to several literatures, its provisions concerning cyberspace are particularly promising. To be more precise, it goes some way toward correcting a significant gap in the research on the development of cyberspace. As I have indicated earlier, substantial effort has been expended describing and investigating the processes by which the Internet was brought to heel under the rule of law. Furthermore, there is a growing body of work on its process of regulation. However, little literature actually conceptualizes its processes of transformation in terms of the issue of securitization and the role that other actors and agencies may play. The current work has shown that the Internet was subject to a broad and profound process of transformation that did not feature the state as a central player, and that the strategies and tactics of securitization which were applied to it had effects that are neither mundane nor inconsequential. Such a finding clearly underscores the need for further work and the importance of redressing this gap in the literature.

Another (and related) contribution made by the work in regard to cyberspace was primarily of a corrective nature. Indeed, against the current theoretical tendency to presuppose cyberspace as an object, the current work mobilized a processual approach thereby foregrounding the constitution of cyberspace as ongoing and open-ended. This approach brought the social character and practices by which cyberspace is constituted into clear relief. In this way it exposed both the socially constructed character of cyberspace and the

dividing practices which operate to sustain the social boundaries associated with its ongoing constitution as a separate place. This procedure proved particularly rewarding where we were examining contexts of emplacement. In this case, the processual focus brought the regimes of para-technical practices associated with securing children in cyberspace into clear focus.

The work also makes several helpful contributions to the social construction of technology tradition. Scholars working in this field have lamented the lack of research addressed to understanding how processes of design and development are inflected with and influenced by broader social, political, and economic background contexts. Thinkers in this tradition reject the idea that processes of problematization have their origin in internal logics of scientific discovery or arise as a consequence of disinterested innovation, setting themselves two more general questions instead: 'why this problematization and why this solution?' In the analysis developed here I have argued that the formation of the securing-child-safety-in-cyberspace problematic was linked to both the strains engendered within neo-liberal rationalities of rule where children are the object of governance and anxieties about technological change characteristic of risk societies. Furthermore, I have argued that an understanding of the twin sources of tension and the way that they may interact provides a perspicacious vantage from which to make sense of the motivational context underlying a variety of initiatives in contexts of design, operations and emplacement. I have not argued, of course, that securitization strategies work to the detriment or exclusion of either approach based on juridification or

regulation.[192] I do contend, however, that the distinguishing feature of securitization as a solution is that it takes strategic aim at the condition of possibility for risk and that the logics associated with this mode of strategic address are deeply connected to neo-liberal modes of rule and risk rationalities.

Another contribution, also related to SCOT, consisted in sketching a conceptual approach which would more clearly expose and render susceptible to analysis the manifestly value laden character of processes of problematization in relation to technological design and development. In particular, the framework developed in the current investigation showed that we need to have a broader understanding of the spectrum of relevant social groups involved in problematizing technological impact, of their political commitments, and of how these may influence future courses of technological development. Through the use of the modified social construction of technology approach, it became clear that the existence of a broad problematic in regard to security was not guarantee of uniformity in terms of interpretation. The security problematic emerged and was addressed within these processes of social construction.

A further, more general contribution of the work was to create a number of connections between thinkers working in the social construction of technology approach and those working within the governmentality approach and risk perspectives. Rather than attempting to build broad conceptual bridges in the abstract, however, the work proceeded instead by building from the ground up in an effort to examine whether, and how, macro-level forces and meso-level logics

---

[192] In fact, I think there are basic complementarities between these different logics, though this is not axiomatic.

are implicated in micro-level contexts. It did this by first introducing the concept of securitization as a meso-level concept which described a generalized logic of neo-liberal modes of risk management – and by tracing the arc of this logic across engineering, operations, and emplacement contexts. At the conceptual level, the work identified three strategies distinct to each domain. In contexts of design, it showed how securitization strategies focus on embedding. In contexts of operation, securitization strategies are interventionist or intermediary in orientation. In contexts of emplacement, securitization is operationalized largely through logics of responsibilization.

Finally, the investigation was intended to open the way for an exploration of a domain of relations and a region of problems that has been largely neglected. Since its advent, the Internet has served as a principal site and battleground for a colossal fight between proponents of free speech on the one hand, and on the other hand those who believe that conduct and content in cyberspace must be subject to some control, whether it be through regulation, legislation or technology. The struggles in the public sphere and in relation to the actions of the state have been well studied by scholars. A key purpose of the current study was to call attention to a parallel processes that has unfolded in an ongoing way in response to a more specific set of worries associated with the welfare of children. Although these processes have mostly advanced below the threshold of public perception, their impact has been at least as redoubtable as the debates raging high above. The discovery and exposure of this secondary and parallel process underscores the continuing importance of Foucault's

contention that we have not yet 'cut off the head of the King' in so far as it shows that sociological and criminological research on cyberspace has been overwhelmingly state-centric and that it has been predominantly negative, focusing on the prohibitive power of law rather than positive forms of power and their diffusion. In this context, the work showed not only that securing cyberspace has not principally or even ultimately been seen as a matter of fighting cyber-crime or even for that matter, about enforcing the law: rather it showed that it has advanced principally through the construction of networks, the development of manuals, the organization of conferences, the definition of terms, and the assembly of curriculum kits.

8.4 Directions for Further Research

This current investigation was highly successful from a heuristic standpoint in so far as it exposed a number of critical vistas through which the study of cyberspace might advance, and opened the way for the further study along several lines and across several regions. An exhaustive identification and discussion of all such avenues is not pursued here. However, four central areas of interest that will undoubtedly prove fruitful for further investigation are noteworthy.

First, one key theme that opened up throughout the course of the investigation (but did not receive methodical or sustained attention) was whether and to what extent the struggles of the RSGs involved in the sundry securitization processes described by the work could be interpreted under the broad rubric of

the democratization of technology. From this standpoint, forming an opinion about and engaging in debate about the various means (regulatory, legislative, and/or technical) appropriate to control content and conduct on the Internet is an important part of the process of steering and shaping the mediums development. Two research directions that might be explored in this context are noteworthy. The first concerns claims making with respect to the existence, nature and extent of problems related to technology. We have seen that such claims can form the basis for wide-spread action and technological change. We have also seen, however, that there are often a number of questions about the validity of the claims made by some of the groups involved in securitization processes. This raises the general question about the venues available for the adjudication of claims with respect to technological properties and impacts, and about the processes by which such claims might be adjudicated.

Second and also related to questions of adjudication, this work showed that design questions are not the sole purview of engineering communities where the Internet is concerned, and that disagreements about design were a recurring source of conflict between RSGs. In this context we have a much more open and inclusive process in which a broad variety of players are involved in raising and attempting to redeem claims about what can be done with the existing techno-social configuration. And we also have the same basic questions about the processes of adjudication associated with these claims. Of course, with respect to the both the first and second issues, we should note that critical cyberspaces, wherein such challenges are mounted, are legion on the Internet. The critical

question, however, is whether the force of the better argument will prevail in decision making with respect to the future development of cyberspace. In terms of directions for further research, we might ask how participants in debates about Internet development understand their roles and what kind of importance they attach to their engagement with the issues.

Third, another direction for further research raised by some of the empirical findings relates to the question of relationships that form between relevant social groups. One of the most intriguing questions that began to emerge as the map of nodal networks and connections between the various agencies, players and stakeholder groups involved in responding to the securing-child-safety-in-cyberspace problematic was: how do alliances form between these groups, and what kinds of factors foster solidarity and cooperation? In several cases, some groups complained about not being able to win the support or cooperation of others. For example, Perverted Justice claimed that it had encountered difficulties gaining the support of law enforcement. Similarly, ASACP complained that about the unwillingness of law enforcement to assist or cooperate. Further study into this issue would be of value in helping to conceptualize the kinds of barriers that may arise in terms of the formation of alliances between different organizations and agencies devoted to protecting the security of children in cyberspace and how they may impact on the overall effort. Further research in this regard is also broadly consistent with the call by some policing scholars for studies of the complex nodal character of the sundry networks involved in providing guarantees of security.

A fourth area for further investigation opened up by the current study relates to neo-liberal rationalities and their consequences for the third sector and communities. We have seen previously that vigilantism is one of the emerging trends in relation to the activities of some third sector organizations in cyberspace. We have also seen that some scholars have suggested that the neo-liberal rationalities with respect to law and order may create the conditions of possibility for the development of such organizations to tip from vigilance to vigilantism. Several other phenomena in cyberspace would seem to be reflective of such tipping; perhaps the most prominent are third sector owned and operated pedophile tracking and shaming websites. Further research into these online organizations is necessary in order to arrive at a clear conception of their commitments and actions, and to understand themselves and their actions.

8.5 Open Questions

The analysis at hand has served up some provocative findings both about the nature and extent of attempts to regulate the Internet, and about the governing logics by which this has been achieved. However, some open questions still remain. For example, we might ask what the analysis of the formation of security structures and strategies and policing networks can tell us about the larger gradient of globalization. The trans-territorial character of the Internet did not occupy a focal position in the present study. However, as was indicated, many of the groups involved in intervention and intermediation at the level of operations hail from diverse quarters of the world and there is seldom a

uniform congruence in law between these countries. This fact alone is often enough to push organizations to find some other basic source of solidarity.

Second, it is necessary to note that although repeated questions about the utility and value of risk logics were raised throughout this study, a definitive or critically normative position with respect to the issues was not observed. The question was left open. Of course, several scholars have decried the impoverishing impacts of risk modes of organization. Others argue that risk logics frequently amount to nothing more than precautionary edicts which actually afford little help to individuals in making decisions about courses of action (Sunstein 2001). One of the open questions in this regard, however, is that of alternatives. If we throw off the yoke of risk and its omnivorous logic of calculation, what should we put in its place?

8.6 The Way Forward

Our understanding of the social character of technology and technological development remains limited, and is therefore is limiting. Many commentators have noted that modern societies are disposed to mystify their relations with technology, and that the way that technologies embody and are a product of human values escapes understanding. Others have lamented the tendency to see and treat technology as determinative of social structure and relations. This is particularly troublesome because it may hinder our awareness of the value laden character of decisions taken with respect to design and their social

impacts, as well as our interfering with our understanding of the impact the design of technological systems these may have in contexts of emplacement.

Criminology, like much of social science, remains mired in a modernist paradigm wherein it is difficult, if not impossible, to conceptualize or even adequately apprehend the structuring impact that technology plays in our everyday lives. Some thinkers have traced this problem back to the modern separation between nature and culture. One of the open questions in terms of how to move forward is whether and to what extent it is necessary to begin to fashion a new vocabulary in order to accommodate new ways of thinking about, and making sense of, the techno-social as a distinct ontological realm. Some scholars have suggested that it is necessary to begin to think of human beings as cyborgs and that a new ontology must be developed to acknowledge the extent to which the human sensorium has become indissociable from the devices that mediate our access to the world (Haraway 1991; Brown 2006). Other thinkers imagine a world in which our sentience is supplemented by wetware which provides ready access to archives of data and thus displaces the function of memory.

All of this may seem like the idle musings of futurists, but the fact remains that projections about our future have a decisive effect in structuring the spectrum of possible futures in so far as they shape and mould our ability to imagine other possibilities (Dublin 1992). If the foregoing study has revealed anything, it is that we would do well to locate and treat our choices in relation to design decisions in an explicitly political way, asking more sophisticated

questions than 'who benefits from this type of design, or whose interests are served'? (Foucault 1984), but also 'what kind of effects we can we expect in terms of the impact that this design decision with have on security?' and 'what future demands will this innovation place upon all of us?' Perhaps this would mean adopting an ecological approach to the techno-sphere. In any case, it is a far cry from the two separate parliaments devoted to two separate entities: people and things. Latour may be right. We may need one Parliament that addresses the hybridized character of our 'never modern' world (1993).

References

Adam, Barbara, Ulrich Beck and Joost Van Loon, eds. 2000. *The Risk Society and Beyond: Critical Issues for Social Theory*. London, England: Sage Publications.

Akdeniz, Yaman. 1997. "The Regulation of Pornography and Child Pornography on The Internet." *Journal of Information, Law & Technology* 1:1-38.

Alexander, Sarah, Stan Meuwese and Annemieke Wolthuis. 2000. "Policies and developments relating to the sexual exploitation of children: The legacy of the Stockholm Conference." *European Journal on Criminal Policy Research* 8:479-501.

Altheide, David L. 2002. *Creating Fear: News and the Construction of Crisis*. Hawthorne, NY: Aldine De Gruyter.

Alvesson, Mats and Kaj Skoldberg. 2000. *Reflexive Methodology: New Vistas for Qualitative Research*. London, England: Sage Publications.

Ambert, Anne-Marie. 1986. "The Sociology of Sociology: The Place of Children in North American Sociology." Pp. 11-31 in *Sociological Studies of Child Development*, vol. 1, edited by P. Adler and P. Adler. Greenwich, CT: JAI Press.

Andermatt, Peter and Verena A. Conley. 1993. *Rethinking Technologies*. Minneapolis, MN: University of Minnesota Press.

Ariès, Philippe. 1962. *Centuries of Childhood*. London, England: J. Cape.

Aronowitz, S., B. Martinsons and M. Mesner, eds. 1996. *Technoscience and Cyberculture*. New York: Routledge.

Aronowitz, S. and M. Mesner. 1996. "On Cultural Studies, Science and Technology." Pp. 7-30 in *Technoscience and Cyberculture*, edited by S. Aronowitz, B. Martinsons, and M. Mesner. New York: Routledge.

Austin, Joe. 1998. *Generations of Youth: Youth Cultures and History in Twentieth-Century America*. New York: New York University Press.

Bakardjieva, Maria and Andrew Feenberg. 2000. "Involving the Virtual Subject." *Ethics and Information Technology* 2(4):233–240.

Bakhtin, Mikhail M. 1981. "Discourse in the Novel." Pp. 259-422 in *The Dialogic Imagination: Four Essays*, edited by M. Holquist. Translated by Michael Holquist and Caryl Emerson. Austin, TX: University of Texas Press.

Barnes, B and D. Edge, eds. 1987. *Science in Context: Readings in the Sociology of Science*. Cambridge, MA: M.I.T. Press.

Barney, Darin. 2000. *Prometheus Wired: The Hope for Democracy in the Age of Network Technology*. Sydney, Australia: UNSW Press.

(------.) 2003. "Invasions of Publicity: Digital Networks and the Privatization of the Public Sphere." Pp. 94-122 in *New Perspectives on the Public/Private Divide*, edited by the Law Commission of Canada. Vancouver, Canada: University of British Columbia Press.

Beck, Ulrich. 1997 *The reinvention of politic*. Cambridge, England: Polity Press.

(------.) 1999. *World Risk Society*. Malden, England: Polity Press.

Beck, Ulrich, Anthony Giddens and Scott Lash. 1994. *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order*. Cambridge, England: Polity Press.

Bender, Gretchen and Timothy Druckrey. 1994. *Culture on the Brink: Ideologies of Technology*. Seattle, WA: Bat Press.

Benedikt, Michael L., ed. 1991. *Cyberspace: First Steps*. Cambridge, MA: M.I.T Press.

Beneditti, Paul and Nancy Dehart, eds. 1996. *Forward Through the Rear-view Mirror: Reflections on McLuhan*. Toronto, Canada: Prentice-Hall.

Bennet, Colin. 2001. "Cookies, web bugs, webcams and cue cats: Patterns of surveillance on the world wide web." *Ethics and Information Technology* 3(3):195–208.

Benson, Rodney. 2004. "Bringing the Sociology of Media Back In." *Political Communication* 21(3):275–292.

Berman, Paul S. 2000. "Cyberspace and the state action debate: The cultural value of applying constitutional norms to 'private' regulation'." *University of Colorado Law Review* 71:1263-1310.

Bernstein, Richard. 1976. *Praxis and Action*. Philadelphia, PA: University of Pennsylvania Press.

Berson, Ilene R. 2002. "Grooming Cybervictims: The Psychosocial effects of online exploitation for youth." *Journal of School Science* 2(1):5-18.

Best, Joel. 1999. *Random Violence: How We Talk about New Crimes and New Victims*. Berkeley, CA: University of California Press.

Biebricher, Thomas. 2005. "Habermas, Foucault and Nietzsche: A Double Misunderstanding." *Foucault Studies* 3:1-26.

Bijker, Wiebe E. 2003. "The need for critical intellectuals: A space for STS." *Science, Technology & Human Values* 28(4):443-450.

Bijker, Wiebe E., Thomas P. Hughes and Trevor J. Pinch, eds. 1987. *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology.* Cambridge, MA: M.I.T. Press.

Bloor, David. 1986. *Knowledge and the Social Imaginary.* Chicago, IL: University of Chicago Press.

Blumer, Herbert. 1971. "Social Problems as Collective Behaviour." *Social Problems* 18:298–306.

Boyle, James. 1997. "Foucault in Cyberspace: Surveillance, Sovereignty and Hard Wired Censors." *Cincinnati Law Review* 11(5):27-48.

Bocij, Paul and Leroy McFarlane. 2003. "The Internet: A Discussion of Some New and Emerging Threats to Young People." *The Police Journal* 76:3-13.

Bossard, James H.S. 1948. *Sociology of Child Development.* New York: Harper.

Brown, James. 1994. *Smoke and Mirrors: How Science Reflects Reality.* New York: Routledge.

Brown, Sheila. 2006. "The Criminology of Hybrids: Rethinking Crime and Law in Technosocial Networks." *Theoretical Criminology* 10(2):223-244.

Brenner, Susan and Bert-Jaap Koops. 2004. "Approaches to Cybercrime Jurisdiction." *Journal of High Technology Law* 4:1.

Buchanan, David, Shaw, Susan, Ford, Amy and Merrill Singer. 2003. "Empirical Science Meets Moral Panic: An Analysis of the Politics of Needle Exchange." *Journal of Public Health Policy* 24(3-4):427 – 444.

Burchell, Graham. 1996. "Liberal government and techniques of the self." Pp. 19-36 in *Foucault and political reason: liberalism, neo-liberalism and rationalities of government*, edited by A. Barry, T. Osborne and N. Rose. London, England: UCL Press.

Burchell, Graham, Colin Gordon and Peter Miller, eds. 1991. *The Foucault Effect: Studies in Governmentality.* Chicago, IL: University of Chicago Press.

Burden, Kit and Creole Palmer. 2003. "Internet crime – Cyber Crime – A new breed of criminal?" *Computer Law and Security Report* 19(3):222-227.

Burke, Debra D. 1997. "The criminalization of virtual child pornography: A constitutional question." *Harvard Journal of Legislation* 43:439-472.

Buzan, Barry. 1997. "Rethinking Security after the Cold War." *Journal of Cooperation and Conflict* 32(1):5-28.

Bynum, Terrell Ward. 2005. "Norbert Wiener's Vision: The Impact of the 'Automatic Age' on our Moral Lives." Pp 1-9 in *The Impact of the Internet on our Moral Lives*, edited by R.J. Cavalier. Albany, NY: University of New York Press.

Callon, Michel, John Law and Arie Rip, eds. 1986. *Mapping the Dynamics of Science and Technology: Sociology and Science in the Real World.* London, England: Macmillan Press.

Cappler, Wanda. 2001. "Not Such a Neat Net: Some Comments on Virtual Criminality." *Social and Legal Studies* 10:229-242.

Carver, Terrell. ed. 1991. *The Cambridge Companion to Marx*. Cambridge, England: Cambridge University Press.

Castel, Robert. 1991. "From dangerousness to risk." In *The Foucault Effect: Studies in Governmental Rationality*, edited by G. Burchell, C. Gordon and P. Miller. Chicago, IL: University of Chicago Press.

Castells, Manuel. 1994. *The Informational City.* Oxford, England: Blackwell Publishing.

Clear, Todd and Eric Cadora. 2001. "Risk and community practice." In *Crime, Risk and Justice: The Politics of Crime in Liberal Democracies*, edited by K. Stenson and R.R. Sullivan. Cullompton, England: Willan Publishing.

Cohen, I. Glenn and Jonathan H. Blavin. 2002. "Gore, Gibson and Goldsmith: The Evolution of Internet Metaphors in Law and Commentary." *Harvard Journal of Law & Technology* 16(1):265-285.

Cohen, Stanley. 1972. *Folk devils and moral panics*. London, England: Mac Gibbon and Kee.

Cooley, Dennis, ed. 2005. *Re-Imagining Policing in Canada*. Toronto, Canada: University of Toronto Press.

Cooper, David. 1995. "Technology: Liberation or Enslavement." In *Philosophy and Technology*, edited by R. Fellows. Cambridge, England: Cambridge University Press.

Cornwell, Benjamin and Annulla Linders. 2002. "The myth of 'moral panic': an alternative account of LSD prohibition." *Deviant Behavior* 23(4):307 – 330.

Davidson, Arnold. 2001. *The Emergence of Sexuality: Historical Epistemology and the Formation of Concepts*. Cambridge, MA: Harvard University Press.

Davies, Simon. 1996. "Surveying Surveillance: An Approach to Measuring the Extent of Surveillance." In *Surveillance, Computers and Privacy* edited by D. Lyon and E. Zureik. Minneapolis, MN: University of Minnesota Press.

Davis, J.C. 1986. *Fear, Myth, and History: The Ranters and The Historians.* Cambridge, England: Cambridge University Press.

Deisman, W.W., R. McLeod, M. Tyrell, and R. Lee. 1996. "Contradictions in Cyberspace." In *Cultures of Internet*, edited by R. Sheilds. London, England: Sage Publications.

Dean, Mitchell. 1999. "Risk, Calculable and Incalculable." In *Risk and Sociocultural Theory*, edited by D. Lupton. Cambridge, England: Cambridge University Press.

(------.) 1999. *Governmentality: Power and Rule in Modern Society*. London, England: Sage Publications.

(------.) 2004. "Four Theses on the Powers of Life and Death." *Contretemps* 5:16–29.

De Kerckhove, Derrick. 1995. *The Skin of Culture: Investigating the New Electronic Reality*. Toronto, Canada: Somerville House Publishing.

Demetriou, Christina and Andrew Silke. 2003. "A Criminological Internet Sting: Experimental Evidence of Illegal and Deviant Visits to a Website Trap." *Britain Journal of Criminology* 43(1):213-222.

Denning, Dorothy E. and William E. Baugh. 1999. "Hiding Crimes in Cyberspace." *Information, Communication and Society* 2(3):251-276.

Dery, Mark, ed. 1993. *Flame Wars: The Discourse of Cyberculture*. Durham, NC: Duke University Press.

Dickson, David. 1984. *The New Politics of Science*. New York: Pantheon.

DiFazio, William. 1996. "Technoscience and the Labour Process." In *Technoscience and Cyberculture,* edited by S. Aronowitz and B. Martinsons. New York: Routledge.

DiMaggio, Paul, Eszter Hargittai, W. Russell Neuman and John P. Robinson. 2000. "Social Implications of the Internet." *Annual Review of Sociology* 27:307-336.

Dixon, Ruth. 1999. "The relationship of hotlines with law enforcement: The IWF Experience." Presented at the Combating Child Pornography on the Internet Conference, September, Vienna, Austria.

Douglas, Mary and Aaron Wildevsky. 2004. *Risk and Culture*. London, England: Routledge.

Doyle, Aaron. 2003. *Arresting Images: Crime and Policing in Front of the Television Camera*. Toronto, Canada: University of Toronto Press.

Dreyfus, Hubert. 1987. Foreword to *Michel Foucault: Mental Illness and Psychology.* Los Angles, CA: University of California Press.

Druckrey, Timothy. 1994. "Introduction." Pp 1-14 in *Culture on the Brink: Ideologies of Technology*, edited by G. Bender and T. Druckrey. Seattle, WA: Bat Press.

Dublin, Max. 1986. *FutureHype: The Tyranny of Prophecy*. New York: Plume.

Durkin, Keith F. 1997. "Misuse of the Internet by pedophiles: Implications for law enforcement and probation practice." *Federal Probation* 61(3):14-18.

Eichmann, David. 1994. "Ethical web agents." Pp 3-13 in *Second International World-Wide Web. Conference: Mosaic and the Web* Chicago, IL.

Ellul, Jacques. 1964. *The Technological Society*. New York: Vintage.

Ericson, Richard V., Patricia M. Baranek and Janet B.L. Chan. 1987. *Visualizing Deviance: Study of News Organization*. Toronto, Canada: University of Toronto Press.

Ericson, Richard V. and Kevin Haggerty. 1997. *Policing the Risk Society*. Toronto, Canada: University of Toronto Press.

Ericson, Richard V. 2006. *Crime in an Insecure World.* Cambridge, England: Polity Press.

Estes, Richard J. 2001. "The sexual exploitation of children: A working guide to the empirical literature." University of Pennsylvania, Center for Youth Policy

Studies. http://caster.ssw.upenn.edu/~restes/CSECFiles/CSEC_Bib_August_2001.pdf

European Commission. 1998. "Commission Communication (Com (97) 570 Final)." Retrieved July 11, 2002 from (http://ec.europa.eu/comm/avpolicy/docs/reg/minors/comlv-en.htm).

Farr, James. 1991. "Science: Realism, criticism, history." Pp 106-123 in *The Cambridge Companion to Marx*, edited by T. Carver. Cambridge, England: Cambridge University Press.

Feenberg, Andrew and Alastair Hannay. 2005. *Technology and the Politics of Knowledge*. Indianapolis, IN: Indiana University Press.

Feenberg, Andrew. 1994. *Critical Theory of Technology.* Oxford, England: Oxford University Press.

(------.) 1999. *Questioning Technology.* New York: Routledge.

Fellows, Roger, ed. 1995. *Philosophy and Technology*. Cambridge, England: Cambridge University Press.

Feyerabend, Paul. 1991. *Three Dialogues on Knowledge*. Oxford, England: Basil Blackwell.

Finkelhor, David, Kimberly J. Mitchell, and Janis Wolak. 2000. "Online victimization: A report on the nation's youth." National Centre for Missing and Exploited Children. Retrieved September 6, 2003 from (http://www.ncmec.org/en_US/publications/NC62.pdf).

Finlay, Markie. 1987. *Powermatics: A Discursive Critique of New Technology.* London, England: Routledge & Kegan Paul.

Florence, Maurice. 1994. "Foucault, Michel, 1926-." Pp 314-320 in *The Cambridge Companion to Foucault*, edited by G. Gutting. Cambridge, England: Cambridge University Press.

Fleck, Ludwik. 1979. *Genesis and Development of a Scientific Fact.* Chicago, IL: University of Chicago Press.

Foucault, Michel. 1977. *Discipline and Punish: The Birth of the Prison.* 2nd ed. New York: Vintage Books.

(------.) 1980. *Power/Knowledge: Selected Interviews and Other Writings 1972-1977*, edited by C. Gordon. New York: Pantheon Books.

(------.) 1981. "Omnes et Singulatim: Towards a Criticism of 'Political Reason'." In *The Tanner Lectures on Human Values*, vol. 2, edited by S. McMurrin. Cambridge, England: Cambridge University Press.

(------.) 1982. "The Subject and Power." Pp. 208-226 in *Michel Foucault: Beyond structuralism and hermeneutics*, edited by H.L. Dreyfus and P. Rabinow. Chicago, IL: University of Chicago Press.

(------.) 1991. "Governmentality." Pp. 87-104 in *The Foucault Effect: Studies in Governmentality*, edited by G. Burchel, C. Gordon and P. Miller. London, England: Havester-Wheatsheaf.

(------.) 1997. "What is Enlightenment?" Translated by Catherine Porter. Pp. 303-329 in *Ethics, Subjectivity and Truth: Essential Works of Michel Foucault 1954-1984*, vol. 1, edited by P. Rabino. New York: The New Press.

(------.) 1998. "Structuralism and Post-Structuralism." Translated by Jeremy Harding. Pp. 431-458 in *Aesthetics, Method and Epistemology: Essential works of Foucault, 1954-1984*, vol. 2, edited by J.D. Faubion. New York: The New Press.

(------.) 1999. *Aesthetics, Method and Epistemology.* New York: The New Press.

(------.) 2003. *Society Must Be Defended: Lectures at the College de France, 1975-1976.* Translated by Doreen Massey. New York: Picador.

(------.) 2006. *The Hermeneutics of the Subject.* Translated by Graham Burchell. New York: Picador.

Fournier de Saint Maur, Agnes. 1999. "The sexual abuse of children via the Internet: A new challenge for Interpol." Presented at the Combating Child Pornography on the Internet Conference, September, Vienna, Austria.

Fry, John. 1975. *Marcuse: Dilemma and Liberation.* Sussex, NJ: Humanities Press.

Gandy, Oscar H. 2003. "Coming to Terms with the Panoptic Sort." Pp. 132-155 in *Surveillance, Computers and Privacy*, edited by D. Lyon and E. Zureik. Minneapolis, MN: University of Minnesota Press.

Garland, David. 2001. "The New Culture of Crime Control." Pp. 171-173 in *The Culture of Social Control.* Chicago, IL: University of Chicago Press.

Geist, Michael. 2002. *Internet Law in Canada.* 3rd ed. Toronto, Canada: Captus Press.

Gerlach, Neil and Sheryl N. Hamilton. 2002. "Virtually Civil: Studio XX, Feminist Voices, and Digital Technology in Canadian Civil Society." Pp. 201-215 in *Civic Discourse and Cultural Politics in Canada: A Cocophony of Voices*, edited by S. Devereaux Ferguson and L. R. Shade. Westport, CT: Ablex Publications.

Giddens, Anthony. 1971. *Capitalism and Modern Social Theory.* Cambridge, England: Cambridge University Press.

(------.) 1990. *Consequences of Modernity.* Stanford, CA: Stanford University Press.

Glaser, Barney G. and Anslem L. Strauss. 1967. *The discovery of grounded theory: Strategies for qualitative research.* Chicago, IL: Aldine Press.

Golding, Peter. 2000. "Forthcoming Features: Information and Communications Technologies and the Sociology of the Future." *Sociology* 34(1):165-184.

Goode, Erich and Nachman Ben-Yehuda. 1994. *Moral Panics: The Social Construction of Deviance.* Cambridge, MA: Blackwell Publishing.

Grabosky, Peter N. and Russell G. Smith. 2001. "Digital Crime in the Twenty-First Century." *Journal of Information Ethics* 10:8 – 26.

Grant, Anna, Fiona David and Peter Grabosky. 1997. "Child pornography in the digital age." *Transnational Organized Crime* 3(4):171-188.

Greenleaf, Graham. 2003. "An endnote on regulating cyberspace: Architecture vs. law?" Pp. 89-120 in *Cyberspace Crime*, edited by D.S. Wall. Aldershot, England: Ashgate Publishing.

Gutstein, Donald. 1999. *E.con: How the Internet Undermines Democracy.* Toronto, Canada: Stoddart Publishing.

Habermas, Jurgen. 1968. *Toward a Rational Society.* Cambridge, MA: M.I.T. Press.

(------.) 1987. "The theory of communicative action." Translated by Thomas McCarthy. In *Lifeworld and system: A critique of functionalist reason*, vol. 2. Boston, MA: Beacon Press.

Hacking, Ian. 2002. *Historical Ontology.* Cambridge, MA: Harvard University Press.

Haggerty, Kevin D. and Richard V. Ericson. 2000. "The Surveillant Assemblage." *British Journal of Sociology* 51:605-622. *Policing the Crisis: Mugging, The State, and Law and Order.* London, England: Macmillan.

Hall, Stuart, Chritcher, Charles, Jefferson, Tony, Clake, John and Brian Roberts. 1978.

Han, Beatrice. 2002. *Foucault's Critical Project: Between the Transcendental and the Historical.* Translated by Edward Pile. Stanford, CA: Stanford University Press.

Haraway, Donna. 1990. "A Manifesto for Cyborgs: Science, Technology and Socialist Feminism in the 1980's." Pp. 190-233 in *Feminism/Postmodernism*, edited by L. Nicholson. New York: Routledge.

(------.) 1997. *Simians, Cyborgs, and Women: The Reinvention of Nature.* New York: Routledge.

Hardison, O.B. 1989. *Disappearing Through the Skylight: Culture and Technology in the Twentieth Century.* New York: Viking Publishing.

Harre, Rom. 1986. *Varieties of Realism.* Oxford/New York: Basil Blackwell.

Heidegger, Martin. 1962. *Being and Time.* San Francisco, CA: Harper-Collins Publishing.

(------.) 1977. *The Question Concerning Technology and Other Essays.* New York: Harper Torch Books.

Heim, Michael. 1993. *The Metaphysics of Virtual Reality.* New York: Oxford University Press.

Hermer, J., M. Kempa, C. Shearing, P. Stenning, and J. Wood. "Policing in Canada in the Twenty-First Century." Pp. 22-91 in *Re-Imagining Policing in Canada: Directions for Law Reform*, edited by D. Cooley. Toronto: University of Toronto Press.

Hindess, Barry. 1996. "Liberalism, socialism, and democracy: Variations on a governmental theme." Pp. 65-80 in *Foucault and political reason: liberalism, neo-liberalism and rationalities of government*, edited by A. Barry, T. Osborne, and N. Rose. London, England: UCL Press.

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

Hinduja, Sameer. 2004. "Perceptions of local and state law enforcement concerning the role of computer crime investigative teams." *Policing: An International Journal of Police Strategies & Management* 27(3):341-357.

Holland, Gemma. 1999. "An analysis of child pornography." Proceedings of the Second COPINE Conference, April, Brussels, Belgium. Unpublished Report.

Honneth, Axel. 1993. *The Critique of Power: Reflective Stages in a Critical Social Theory*. Cambridge, MA: M.I.T. Press.

Howitt, Dennis. 1995. "Pornography and the pedophile: Is it criminogenic?" *British Journal of Medical Psychology* 68:15-27.

Huey, Laura J. 2002. "Policing the abstract: Some observations on policing cyberspace." *Canadian Journal of Criminology* 44(3):243–254.

Hughes, Tom. 1986. "Uncited Sources." *Technology and Culture* 27:570-576.

Hunt, Alan. 1999. "The Purity Wars: Making Sense of Moral Militancy." *Theoretical Criminology* 3(4):409-436.

Iannotta, Joah G. 2001. *Nontechnical Strategies to Reduce Children's Exposure to Inappropriate Material on the Internet*. Washington, D.C.: National Academy Press.

Idhe, Don. 1986. *Consequences of Phenomenology.* Albany, NY: State University of New York Press.

(------.) 1983. *Existential Techniques*. Albany, NY: State University of New York Press.

Innes, Martin. 2003. *Understanding Social Control: Deviance, Crime and Social Order.* Berkshire, England: Open University Press.

Jackson, Stevi and Sue Scott. 1991. "Risk Anxiety and the Social Construction of Childhood." Pp. 86-107 in *Risk and Sociocultural Theory*, edited by D. Lupton. Cambridge, England: Cambridge University Press.

Jagtenberg, Tom. 1983. *The Social Construction of Science: A Comparative Study of Goal Direction, Research Evolution and Legitimation*. London, England: D. Reidel Publishing Company.

Jenkins, Philip. 1998. *Moral Panic: Changing concepts of the child molester in modern America*. New Haven, CT: Yale University Press.

(------.) 1999. *Synthetic Panics: The Symbolic Politics of Designer Drugs.* New York: New York University Press.

(------.) 2001. *Beyond Tolerance: Child pornography on the Internet.* New York: New York University Press.

Johnston, Les D. and Clifford D. Shearing. 2003. *Governing Security: Explorations in Policing and Justice.* New York: Routledge.

Kellner, Douglas. 1989. *Critical Theory, Marxism and Modernity.* Cambridge, England: Polity.

Kempa, Michael, Ryan Carrier, Jennifer Wood and Clifford D. Shearing. 1999. "Reflections of the Evolving Concept of 'Private Policing'." *European Journal on Criminal Policy and Research* 7(2):197-223.

Kim, Junghoon and Tomoaki Watanabe. 2001. The Social Construction of the Internet and Emerging Problems of Internet Governance. GRICS Conference, Montreal, April 24.

Kingwell, Mark. 1996. *Dreams of the Millennium* Toronto, Canada: Penguin Group.

Kinney, Jay. 1996. "Is There a New Political Paradigm Lurking in Cyberspace?" Pp. 138-153 in *Cyberfutures: Culture and Politics on the Information Superhighway*, edited by Z. Sadar and J. Ravetz. New York: New York University Press.

Kinsman, Gary, Dieter Buse and Mercedes Steedman, eds. 2002. *Whose National Security: Canadian State Surveillance and the Creation of Enemies.* Toronto, Canada: Between the Lines Press.

Klein, H. K. and D.L. Kleinman. 2002. "The Social Construction of Technology: Some Structural Considerations." *Science, Technology & Human Values* 27(1):28-52.

Kline, Ronald and Trevor Pinch. 1996. "Users as agents of technological change: The social construction of the automobile in the rural United States." *Technology and Culture* 37(4):763-795.

Kleinknecht, Steven. 2000. "Borders Conference - Rethinking the Line: The Canada-U.S. Border / Child Pornography on the Internet Session." Ottawa, Canada: Research and Statistics Division, Department of Justice Canada.

Kovacich, Gerald L. and William C. Boni. 2000. *High-Technology-Crime Investigator's Handbook: Working in the Global Information Environment.* Woburn, MA: Butterworth Heineman.

Kroker, Arthur. 1996. "Virtual Capitalism." Pp 167-180 in *Technoscience and Cyberculture*, edited by S. Aronowitz, B. Martinsons, and M. Mesner. New York: Routledge.

(------.) 1994. *Data Trash: The Theory of the Virtual Class*. Montreal, Canada: New World Perspective.

Kurzweil, Raymond. 1990. *The Age of Intelligent Machines*. Cambridge, MA: M.I.T. Press.

Latour, Bruno. 1987. *Science in Action*. Cambridge, MA: Harvard University Press.

(------.) 1996. *Aramis, or the Love of Technology*. Translated by Catherine Porter. Cambridge, MA: Harvard University Press.

(------.) 1993. *We Have Never Been Modern*. Cambridge: Harvard University Press.

Latour, Bruno and Steve Woolgar. 1977. *Laboratory Life: The Construction of Scientific Facts*. London, England: Sage Publications.

Layton, E.T. 1977. "Conditions of Technological Development." Pp.197-222 in *Science, Technology and Society: A Cross-disciplinary Perspective*, edited by I. Spiegel-Rösing and D. de Solla Price. London, England: Sage Publications.

Lemke, Thomas. 2001. Foucault, Governmentality, and Critique. Presented at the Rethinking Marxism Conference, September, Amherst, MA.

Lemos, Andre. 1996. "The Labyrinth of Minitel". In *Cultures of Internet,* edited by R. Shields. London, England: Sage Publications.

Lessig, Lawrence. 2000. *Code and Other Laws of Cyberspace*. New York: Basic Books.

Le Toquin, Jean-Christophe. 1999. "Guidelines for codes of conduct." Presented at the Combating Child Pornography on the Internet Conference, September, Vienna, Austria.

Lewis, James Andrew. 2005. "Aux armes, citoyens: Cyber security and regulation in the United States." *Telecommunications Policy* 29:821–830.

Lianos, Michaelis and Mary Douglas. 2000. "Dangerization and the End of Deviance: The Institutional Environment." *British Journal of Criminology* 40(3):264–78.

Little, Daniel. 1986. *The Scientific Marx*. New York: Cornell University Press.

Lupton, Deborah, ed. 1999. *Risk and Sociocultural Theory: New Directions and Perspectives*. Cambridge, England: Cambridge University Press.

Lyon, David and Elia Zureik. 1996. *Surveillance, Computers and Privacy*. Minneapolis, MN: University of Minnesota Press.

MacGillavry, E. 1999. "Internet service providers and criminal investigations: A case study regarding the voluntary co-operation of Dutch ISPs with the investigating authorities." Presented at the Combating Child Pornography on the Internet Conference, September, Vienna, Austria.

Machill, Marcel and Jens Waltermann. 1999. *Self-Regulation of Internet Content*. Germany: Bertelsmann Foundation.

MacKenzie, Donald and Judy Wajcman, eds. 1999. *The Social Shaping of Technology*. 2nd ed. Philadelphia, PA: Open University Press.

MacNeill, Michael, Neil Sargent and Peter Swan. 2002. *Law, Regulation and Governance*. Toronto, Canada: Oxford University Press.

Marx, Gary T. 1996. "Electric Eye in the Sky: Some Reflections on the New Surveillance and Popular Culture." In *Surveillance, Computers and Privacy*, edited by D. Lyon and E. Zureik. Minneapolis, MN: University of Minnesota Press.

Marx, Karl. 1970. *The German Ideology*. New York: International Publishers.

Matick, Paul. "Limits of Interrogation." In *The Critical Spirit: Essays in Honour of Herbert Marcuse*, edited by K. H. Wolff and B. Moore Jr. Boston, MA: Beacon.

McCarthy, Thomas. 1998. *Habermas and Critical Theory*. Cambridge, MA: M.I.T. Press.

McCune, M. Megan. 2002. "Virtual Lollipops and Lost Puppies: How Far can States Go to Protect Minors Through the Use of Internet Luring Laws." *Commonlaw Conspectus* 14:504.

McCabe, Kimberly A. 2002. "An Assessment of Child Pornography via Internet Newsgroups: Identifying Change in the Last Five Years." Southern Sociological Society.

McLuhan, Marshall and Bruce Powers. 1994. *The Global Village: Transformations in World Life and Media in the 21st Century*. New York: Oxford University Press.

McLuhan, Marshall and Eric McLuhan. 1998. *Laws of Media: The New Science*. Toronto, Canada: University of Toronto Press.

McLuhan, Marshall. 1964. *Understanding Media: The Extensions of Man*. New York: Penguin Group.

McRobbie, Angela and Sarah L. Thornton. 1995. "Rethinking 'Moral Panic' for Multi-Mediated Social Worlds." *The British Journal of Sociology* 46(4):559 – 574.

Mead, George Herbert. 1972. *The Philosophy of the Act*. Chicago, IL: University of Chicago Press.

Media Awareness Network. 2004. "Web Aware." Retrieved April 26, 2004 (www.bewebaware.ca).

Mesner, Michael. 1996. "Becoming Heterarch: On Technocultural Theory, Minor Science and the Production of Space". Pp 293-316 in *Technoscience and Cyberculture*, edited by S. Aronowitz, B. Martinsons, and M. Mesner. New York: Routledge.

Mosco, Vincent and Janet Wasko. 1998. *The Political Economy of Information.* Madison, WI: University of Wisconsin Press.

Moyer, S. 1992. "Working document: A preliminary investigation into child pornography in Canada." Ottawa, Canada: Research and Development Directorate, Department of Justice Canada.

Mulkay, Michael. 1972. *The Social Processes of Innovation: A Study in the Sociology of Science*. London, England: Macmillan Press.

(------.) 1979. *Science and the Sociology of Knowledge.* London, England: George Allen and Unwin.

(------.) 1991. *Sociology of Science: A Sociological Pilgrimage*. Buckingham, England: Open University Press.

Murphy, Chris and Curtis Clark. 2002. "Policing Communities and Communities of Policing: A Comparative Study of Policing and Security in Two Canadian Communities." Pp. 209-259 in *Re-Imagining Policing in Canada: Directions for Law Reform*, edited by D. Cooley. Toronto, Canada: University of Toronto Press

Netanel, Neil Weinstock. 2000. "Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory." *California Law Review* (88)2:395-498.

Norris, Clive and Gary Armstrong. 1999. "The Maximum Surveillance Society: The Rise of CCTV." New York: Oxford University Press.

Nelkin, Dorthy. 1996. "Perspectives on the Evolution of Science Studies." Pp. 31-36 in *Technoscience and Cyberculture*, edited by S. Aronowitz, B. Martinsons, and M. Mesner. New York: Routledge.

Nye, Andrea. 1994. *Philosophia: The Thought of Rosa Luxemburg, Simone Weil and Hanna Arendt.* London, England: Routledge.

Olsen, W. 2004. "Triangulation in Social Research: Qualitative and Quantitative Methods Can Really Be Mixed." In *Developments in Sociology*, edited by M. Holborn. Ormskirk, England: Causeway Press.

O'Malley, Pat. 2001. "Policing crime risks in the neo-liberal era." Pp. 89-103 in *Crime, Risk and Justice: The Politics of Crime in Liberal Democracies*, edited by K. Stenson and R.R. Sullivan. Cullompton, England: Willan Publishing.

Ogburn, William. 1964. *On Culture and Social Change.* Chicago: The University of Chicago Press

Panzieri, Raniero. 1980. 'The Capitalist Use of Machinery: Marx Versus the Objectivists." In *Outlines of a Critique of Technology*, edited by P. Slater. London, England: Ink Links.

Parsons, Talcott. 1966. *Societies.* Englewood Cliffs, NJ: Prentice-Hall.

(------.) 1951. *The Social System.* New York: Free Press.

Pickering, Andrew. 1979. *The Mangle of Practice: Time, Agency and Science.* Chicago, IL: Chicago University Press.

Pinch, Trevor J. and Wiebe E. Bijker. 1984. "The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other." *Social Studies of Science* 14:399-441.

(------.) 1986. "Science, Relativism and the New Sociology of Technology: Reply to Russell." *Social Studies of Science* 16:347-360.

Platt, Charles. 1991. *The Silicon Man.* New York: Bantam.

Popper, Karl. 1972. *Objective Knowledge.* Oxford, England: Oxford University Press.

(------.) 1961. *The Poverty of Historicism.* New York: Harper Row.

Poster, Mark. 1990. *The Mode of Information: Poststructuralism and Social Context.* Chicago, IL: University of Chicago Press.

Postman, Neil. 1992. *Technopoly*. New York: Alfred A. Knopf.

Powel, Jason L. and Margaret Edwards. 2003. "Risk and youth: A critical sociological narrative." *International Journal of Sociology and Social Policy* 23(12):81-94.

Price, Monroe E. and Stefaan G. Verhulst. 2000. "In search of the self: Charting the course of self-regulation on the Internet in a global environment." Cardozo Law School. Unpublished paper.

Quayle, Ethel and Max Taylor. (2001). "Child seduction and self-representation on the Internet: A case study." *CyberPsychology and Behavior*, 4(5), 597-608.

(------.) 2003. "Model of Problematic Internet Use in People with a Sexual Interest in Children." *CyberPsychology and Behavior* 6(1):93-106.

Rabinow,Paul and Nikolas Rose, eds. 2003. *The Essential Foucault: Selections from Essential Works of Foucault 1954-1984.* New York: New Press.

Racicot, Michel, MarkS. Hayes, Alec R. Szibbo and Pierre Trudel. 1998. "The cyberspace is not a "no-law land": A study of liability for content circulating on the Internet." *Computer Law and Security Report* 14(2):96-106.

Ravetz, Jerome. 1996. "The Microcybernetic Revolution and the Dialectics of Ignorance." Pp. 42-60 in *Cyberfutures: Culture and politics on the Information Superhighway*, edited by Z. Sardar and J. Ravetz. New York: New York University Press.

Rettinger, Jill L. 2000. "The relationship between child pornography and the commission of sexual offences against children: A review of the literature." Ottawa, Canada: Research and Statistics Division, Department of Justice Canada. Retrieved August 14, 2002 from (http://www.justice.gc.ca/en/ps/rs/rep/2000/rr00-5.html).

Reinfelder, Monika. 1980. "Breaking the Spell of Technicism." Pp. 9-37 in *Outlines of a Critique of Technology* edited by P. Slater. London, England: Ink Links.

Richards, Stewart. 1983. *Philosophy and the Sociology of Science: An Introduction.* London, England: Basil Blackwell.

Rigakos, George S. 2002. *The New Parapolice: Risk Markets and Commodified Social Control.* Toronto, Canada: University of Toronto Press.

Ritzer, George. 1988. *Contemporary Sociological Theory.* 2nd ed. New York: Alfred A. Knopf.

Robinson, Kristopher K. and Edward M. Crenshaw. 2002. "Post-industrial transformations and cyber-space: a cross-national analysis of Internet development." *Social Science Research* 31:334–363.

Rose, Hillary and Steven Rose, eds. 1976a. *The Political Economy of Science: Ideology of/in the Natural Sciences.* London, England: Macmillan Press.

(------.) 1976b. *The Radicalization of Science.* London, England: Macmillan Press.

Rosenberg, Richard S. 2001. "Controlling Access to the Internet: The role of filtering". *Ethics and Information Technology* 3:35-54.

Ross, Andrew. 1989. "Hacking Away at the Counter-Culture". In *Technoculture*, edited by C. Penley and A. Ross. Minneapolis, MN: University of Minnesota Press.

(------.) 1991. *Strange Weather: Culture, Science and Technology in the Age of Limits.* New York: Verso.

Rouse, Joseph. 1987. *Knowledge and Power: Toward a Political Philosophy of Science.* Ithaca, NY: Cornell University Press.

Russell, Stewart. 1986. "The Social Construction of Artifacts: Response to Pinch and Bijker." *Social Studies of Science* 16:331-346.

Salter, Anna C. 2003. *Predators: Pedophiles, Rapists, and Other Sex Offenders: Who They Are, How They Operate, and How We Can Protect Ourselves and Our Children.* New York: Basic Books.

Salter, Lee. 2005. "Colonization tendencies in the development of the world wide web." *New Media & Society* 7(3):291-309.

Schehr, Robert C. 2005. "Conventional risk discourse and the proliferation of fear." *Criminal Justice Policy Review* 16(1):38-58.

Scheibler, Ingrid. 1993. "Heidegger and the Rhetoric of Submission." In *Re-Thinking Technologies*, edited by V. A. Conley. Minneapolis, MN: University of Minnesota Press.

Scott, Sue, Stevi Jackson and Kathryn Backett-Milburn. 1998. "Swings and Roundabouts: Risk Anxiety and the Everyday Worlds of Children." *Sociology* 32:689-705.

Secretariat of the Asia Pacific Forum of National Human Rights Institutions. 2000. "Term of Reference on Child Pornography on the Internet – Background Paper". Prepared for the Advisory Council of Jurists, Asia Pacific Forum of National Human Rights Institutions. Unpublished Report.

Shallis, Michael. 1991. "The Silicon Idol." In *Questioning Technology: Tool, Toy or Tyrant?* edited by J. Zerzan and A. Carnes. Philadelphia, PA: New Society.

Shapiro, Andrew. 1999. *The Control Revolution: How the Internet is Putting People in Charge and Changing the World We Know*. New York: Public Affairs.

Shearing, Clifford D. 1992. "The Relationship Between Public and Private Policing." Pp. 399-434 in *Modern Policing*, edited by M. Tony and N. Morris. Chicago, IL: University of Chicago Press.

(------.) 2003. "Preface." Pp. xvii to xviii in *Selling Security: The Private Policing of Public Space*, by Alison Wakefield. Cullompton, England: Willan Publishing.

Shearing, Clifford D. and M. Kempa. 2000. "Rethinking the Governance of Security in Transitional Democracies." *Nigerian Law Enforcement Review* 33–37.

Shearing, Clifford D. and P. Stenning, eds. 1981. "Modern Private Security: Its Growth and Implications." Pp. 193-245 in *Crime and Justice: An Annual Review of Research*, edited by M. Tonry and N. Morris, vol. 3. Chicago, IL: University of Chicago Press.

(------.) 1983. "Private Security: Implications for Social Control" *Social Problems* 30(5):493–506.

(------.) 1987. *Private Policing*. Newbury Park, CA: Sage Publications.

Shearing, Clifford D. and J. Wood. 2003. "Nodel Governance, Democracy and the New Denizens." *Journal of Law and Society* 30(3):400–19.

Sheptycki, James W.E., ed. 2000. *Issues in Transnational Policing*. New York: Routledge.

Sieber, Ulrich. 1999. "Responsibility of Internet providers: A comparative legal study with recommendations for future legal policy." Paper presented at the Combating Child Pornography on the Internet conference, September, Vienna, Austria

Sismondo, Sergio. 1993. "Some Social Constructions." *Social Studies of Science* 23:515-553.

Slater, Phil. 1980. *Outlines of a Critique of Technology*. London, England: Ink Links.

Smart, Barry. 1988. *Key Sociologists: Michel Foucault*. New York: Routledge.

Sobchack, Vivian. 1996. "Democratic Franchise and the Electronic Frontier." Pp. 77-89 in *Cyberfutures*, edited by Z. Sadar and J. Ravetz. New York: New York University Press.

Sorrel, Tom. 1996. *Scientism: Philosophy and the Infatuation with Science*. New York: Routledge.

Sparks, Richard. 2001. "Bringin' it all back home': Populism, media coverage and the dynamic of locality and globality in the politics of crime control." Pp. 194-213 in *Crime, Risk and Justice: The Politics of Crime in Liberal Democracies*, edited by K. Stenson and R. R. Sullivan. Cullompton, England: Willan Publishing.

Spector, Malcolm and John I. Kitsuse. 1987. *Constructing Social Problems*. New York: DeGruyter.

Spinello, Richard A. 2002. *Regulating Cyberspace: The Policies and Technologies of Control*. Westport, CT: Quarum Books.

Staudenmaier, John M. 1985. *Technology's Storytellers: Reweaving the Human Fabric*. Cambridge, MA: M.I.T. Press.

Stefik, Mark, ed. 1996. *Internet Dreams: Archetypes, Myths, and Metaphors for Inventing the Net*. Cambridge, MA: M.I.T. Press.

Stenson, K.evin and Adam Edwards. 2001. "Crime control and liberal government: the 'third way' and the return to the local." Pp. 68-86 in *Crime,*

Risk and Justice: The Politics of Crime in Liberal Democracies, edited by K. Stenson and R. R. Sullivan. Cullompton, England: Willan Publishing.

Stenson, Kevin. 2001. "The new politics of crime control." Pp. 15-28 in *Crime, Risk and Justice: The Politics of Crime in Liberal Democracies*, edited by K. Stenson and R. R. Sullivan. Cullompton, England: Willan Publishing.

Stiegler, Bernard. 1996. "Questioning Technology and Time." Translated by Richard Beardsworth. *Teknema: Journal of Philosophy and Technology* 1(1):31-46.

Stone, Allucquere Rosanne. 1992. "Virtual Systems." In *Incorporations (Zone 6)*, edited by J. Crary and S. Kwinter. Cambridge, MA: M.I.T. Press.

(------.) 1996. *The War of Desire and Technology at the Close of the Mechanical Age*. Cambridge, MA: M.I.T. Press.

Stone, Brad Elliott. 2004. "Defending Society From the Abnormal: The Archaeology of Bio-Power." *Foucault Studies* 1:77-91.

Sullivan, Robert R. 2001. "The schizophrenic state: Neo-liberal criminal justice." Pp. 29-48 in *Crime, Risk and Justice: The Politics of Crime in Liberal Democracies*, edited by K. Stenson and R. R. Sullivan. Cullompton, England: Willan Publishing.

Sunstein, Cass R. 2001. *Republic.com.* Princeton, NJ: Princeton University Press.

(------.) 2005. *Laws of Fear: Beyond the Precautionary Principle*. Cambridge, MA: Cambridge University Press.

Sussman, Vic. 1995. "Policing Cyberspace." *U.S. News*, January 23, p.54.

Taniguchi, Megumi I. 2003. "Internet Metaphors Matter." *New Directions for Teaching and Learning* 94:13-21.

Taylor, Max. 2001. "Child pornography and the Internet: Challenges and gaps." Presented as a panel presentation to the 2nd World Congress Against the Sexual Exploitation of Children, December, Yokohama, Japan.

Taylor, Max, Ethel Quayle and Gemma Holland. 2001. "Child pornography, the Internet and offending." *ISUMA: The Canadian Journal of Policy Research*, 2(2):94-100. Retrieved August 19, 2002 from (http://www.isuma.net/v02n02/taylor/taylor_e.shtml).

Thomas, Graham and Sally Wyatt. 1991. "Shaping Cyberspace - interpreting and transforming the Internet." *Research Policy* 28(7).681–698.

Thomas, William I. and Dorothy Swaine Thomas. 1928. *The child in America: Behavior problems and programs*. New York: Alfred A. Knopf.

Thornburgh, Dick and Herbert S. Lin, eds. 2002. *Youth, Pornography, and the Internet*. Washington, D.C.: National Academies Press.

Toffler, Alvin. 1980. *The Third Wave.* New York: Random House.

Touraine, Alain. 1974. *The Post-Industrial Society*. New York: Wildwood House.

Tridgell, Amy. 2000. "Newsgathering and child pornography research: the case of Lawrence Charles Matthews." *Columbia Journal of Law and Social Problems* 33(4):343-390.

Ungar, Sheldon. 2001. "Moral panic versus the risk society: The implications of the changing sites of social anxiety." *British Journal of Sociology* 52(2):271–291.

Valverde, Mariana. 1998. *Diseases of the Will: Alcohol and the Dilemmas of Freedom*. Cambridge, England: Cambridge University Press.

Van Loon, Joost. 2002. *Risk and Technological Culture: Towards a Sociology of Virulence*. New York: Routledge.

Virilio, Paul. 1995. *The Art of the Motor*. Translated by Julie Rose. Minneapolis, MN: University of Minnesota Press.

(------.) 2000. *The Information Bomb*. Translated by Chris Turner. London, England: Verso.

Wall, David S. 1999. "Cybercrimes: New Wine, No Bottles?" Pp. 105-139 in *Invisible Crimes: Their Victims and their Regulation*, edited by P. Davies, P. Francis and V. Jupp. London, England: Macmillan Press.

Webster, Andrew. 1991. *Science, Technology and Society*. New Brunswick, NJ: Rutgers University Press.

Weinberg, Leonard, Ami Pedahzur and Sivan Hirsch-Hoefler. 2004. "The Challenges of Conceptualizing Terrorism." *Terrorism and Political Violence* 16(4):777-794.

Welch, Michael. 2000. *Flag Burning: Moral Panic and the Criminalization of Protest.* Piscataway, New Jersey: Aldine Transaction.

Wickham, Gary and George Pavlich, eds. 2001. *Rethinking Law, Society and Governance: Foucault's Bequest*. Portland, OR: Hart Publishing.

Winner, Langdon. 1980. "Do Artifacts Have Politics?" *Daedalus* 109(1):121-136.

(------.) 1991. "Upon Opening the Black Box and Finding it Empty: Social Constructivism and the Philosophy of Technology." *Science Technology & Human Values* 18(3):362-378.

(------.) 1992. *Democracy in a Technological Society*. Dordrecht, Holland: Kluwer Academic Publishers.

Winsek, Derek. 2002. Netscapes of Power. *Media, Culture & Society* 24: 795–819.

Wolmack, Jenny. 2002. *Cybersexualities: A Reader on Feminist Theory, Cyborgs, and Cyberspace*. Edinburgh, Scotland: Edinburgh University Press.

Woolgar, Steve and Dorthy Pawluch. 1985. "Ontological Gerrymandering." *Social Problems* 32(3):214-227.

Zittran, Jonathan. 2003. "Internet Points of Control." *Boston College Law Review* 44(2):653-688.

Index of Appendices

Appendix A:
Tables of Data Sources by Subject of Analysis

1. List of Empirical Data in Relation to Claims Making Aimed at Representing the Risks – Problematizing Child Safety

	Source	Methodology-Method
Media Reports 1992-2000 Newspapers	Globe and Mail, N*ational Post, St. John's Telegram, Halifax Daily News, Montreal Gazette, Ottawa Citizen, Toronto Star, Regina Leader Post,* E*dmonton Journal, Vancouver Sun* and the *Victoria Times Colonist*	Rudimentary Text Analysis Thematic Discourse Analysis
Advertising and Marketing Products (1995-2000)	Marketing Materials and Packaging: 1. Net Nanny – brochure – website information, secondary advertising on other websites, and packaging. 2. Cyber-watch – brochure, website. 3. Surf Patrol – brochure, website, secondary advertising. 4. Cyber-sitter - brochure, website 5. Safe-surf - website information, secondary advertising on other websites, packaging, commentary on other websites.	Thematic Discourse Analysis aimed at disclosing construction of danger – conceptions of responsible parties.

2. Empirical Data – Design Contexts: Securitization Through Embedding

	States	Private Sector	Third Sector Organizations	Methodology
International and Transnational	n/a	AOL, KOL	Surf-Watch Peacefire Censorware Project	Description, Discourse Analysis
National and Provincial	R.C.M.P O.P.P. Center for Missing and Exploited Children	Canadian Consortium of ISPs,	n/a	Description, Discourse Analysis

3. Empirical Data – Sources on Intermediaries and Interveners

	Between and Within States by State Authorities	Private Sector	Third Sector Organizations
International and Transnational	Interpol COPINE Project Virtual Crime Task Force	n/a	I.C.A.N.N. Perverted Justice Hackers Against Child Pornography Adult Sites Against Child Pornography
National and Provincial	R.C.M.P O.P.P. Center for Missing and Exploited Children I.H.A.C. Publications	Documents from the Internet Service Providers Association, Bell Canada Rogers	

4. Empirical Data – Sources on Responsibilization

	States	Private Sector	Third Sector
International and Trans-national	International Agreements: Convention Against Cybercrime	AOL- End-user Agreements	Online Parents Forums
National	Missing LiveWires Classroom Contracts	Consortium of Internet Service Providers Association	Safe-Surf Canada

Appendix B:

Listing of Selected Primary and Secondary Sources of Data

1. Canadian Government Documents

Canada. (1994) *Order in Council P.C. 1994-1689.*

Canada. Privacy Commissioner. (1994) *Annual Report.* Ottawa: Supply and Services Canada.

Canadian Radio-Television and Telecommunications Commission. (1994) *Telecom Decision 94-1B [Review of Regulatory Framework]* Hull, Quebec: Canadian Radio-Television and Telecommunications Commission.

Industry Canada. (1994b) *The Canadian Information Highway: Building Canada's Information and Communications Infrastructure*. Ottawa: Minister of Supply and Services. Available:

Industry Canada. (1994c) *Government to Proceed with Amendments to Copyright Act* [Industry Canada news release]. Available:

Public Advisory Council on Information Highway Policy. (1994) *The Public Advisory Council on Information Highway Policy's Opposing Intervention in Response to: Notice of Public Hearing CRTC 1994-11 and Related RCI Applications*. Hull, Que: Canadian Radio-Television and Telecommunications Commission. Available: e-mail://ba439@freenet.carleton.ca.

Cyber!Tip.ca. The Identification of Trends of Child Online Sexual Exploitation. An analysis of Reports Received in CyberTips pilot phase 2002-2004. Child Find Manitoba.
Kim Bunzeluk 2005.

Appendix B:

Listing of Selected Primary and Secondary Sources of Data

Third Sector Reports and Papers

Advisory Council of Jurists, Asia Pacific Forum of National Human Rights Institutions 2000. *Terms of Reference on Child Pornography on the Internet – Background Paper* (July).

Berson, I. 2002. Grooming Cybervictims: The Psychosocial effects of online exploitation for youth. In J. Hosking, & H. Broad (Co-chairs), *NetSafe: Society, Safety and the Internet.* [Online]. Symposium conducted in Auckland, New Zealand.

Iannotta, J. G. (2001). Nontechnical Strategies to Reduce Children's Exposure to Inappropriate Material on the Internet. Washington, D.C.: National Academy Press.

Moyer, S. (1992, May). *Working document: A preliminary investigation into child pornography in Canada.* Ottawa: Research and Development Directorate Department of Justice Canada

O'Connor, Rachel (2002) A Typology of Cybersexpolitation and Online Grooming Practices. *Cyberspace Research Unit, University of Central Lancashire.*

Salter, Anna. (2003). Predators: Pedophiles, Rapists, and Other Sex Offenders: Who They Are, How They Operate, and How We Can Protect Ourselves and Our Children/ *New York, Basic Books, 2003, 272 pages, $26*

Williams, Nigel (1999, September) *The Contribution of Hotlines to Combating Child Pornography on the Internet.* Childnet International [Online].

Wishart, J. (2004) Internet safety in emerging educational contexts. *Computers and Education*, Volume 43, Issue 1-2 SPEC ISS., August, Pages 193-204

Barlow, J.P. 1996. Unpublished Manuscript. Available: http://www. eff. org/pub/.

Appendix C:

Sample of American Reporting Categories

Taken from www.obscenitycrimes.org.

Possession, Manufacture, and Distribution of Child Pornography
Child pornography has been defined under federal statute as a visual depiction of a minor (child younger than 18) engaged in sexually explicit conduct (18 U.S.C. 2256).

Online Enticement of Children for Sexual Acts
Use of the Internet to entice, invite, or persuade a child to meet for sexual acts, or to help arrange such a meeting, is a serious offense (18 U.S.C. 2425).

Prostitution of Children
Prostitution is generally defined as performing, offering, or agreeing to perform a sexual act for any money, property, token, object, article, or anything of value (18 U.S.C. 2431, 2423(a)).

Sex Tourism Involving Children
It is against the law for any United States citizen to travel abroad to engage in sexual activity with any child under the age of 18 (18 U.S.C. 2423(b)). Individuals who partake in this illegal activity are subject to prosecution in the United States even if they committed the crime on foreign soil.

Child Sexual Molestation (not in the family)
Child sexual exploitation (not in the family), also known as extra-familial child sexual abuse, includes all sexual exploitation of a child by someone other than a family member.

Unsolicited Obscene Material Sent to a Child
It is an unfortunate reality of the Internet that children will encounter obscene material online. Many times this material is attached as an image(s) or hyperlink(s) sent to a child in an unsolicited E-mail or "spam."

To combat this problem NCMEC takes reports of unsolicited obscene material sent to a child. It is a violation of criminal law for any person to knowingly or attempt to send or transfer obscene material to another individual who has not attained the age of 16 years (18 U.S.C.A. 1470).

Appendix D:

Revenue Flows and for Adult Websites

There are several revenue streams open to site owners: They may use direct advertising through banner ads, select text links, or other creatives. They may use the previously mentioned sponsor-provided galleries that contain an affiliate code giving them credit for any membership sales thus generated (with an average payout of $30-$35 per referred signup). They might collect and sell e-mail addresses, sell items such as 'penis enlargement' products, and also link to live video chat, dating, or adult novelty sites (once again, in hopes of receiving a nice commission check).

The most popular TGP's sell gallery listings to submitters. For example, if a webmaster lists 35 new galleries in a daily update, but receives 300+ submissions from other webmasters hoping to find a slot in that update, the reality that this is a buyer's market hits home, and he can then sell his top x number of slots for y dollars, and use sponsor galleries for filler.

As for being redirected to different sites when you're trying to view a gallery because you like a thumbnail image or provocative text link, there are several possibilities. The worst case is that you have received a virus that is sending you to sites of the creator's choosing, rather than where you're trying to go. Another possibility is that you're hitting what are known as 'blind links' – so rather than going somewhere specific, you're following a generic link such as "Teen Web Cams" which could take you to any site, the choice of which is made by the TGP owner who will get a commission if you join there.

Overwhelmingly, however, the reason that you go to a different gallery post site instead of to the gallery you were trying to visit is because you were "traded." Traffic trades are the primary way in which most of these sites attract visitors. The back-end scripting assigns what is known as a "skim percentage" to the thumbnails and links (all of which are pre-determined by the site owner). Click the thumb three times (for example) and once you might see the gallery, the other two times you'll hit one of that site's trades. The site you end up at records your visit and then sends a surfer back to the referring site. Since new browser windows are typically opened in this process, one visitor to one site might get traded multiple times, returning an equal number of visitors back to the originating site.

This whole traffic trading process is automated, and the scripting quite sophisticated, developed out of the desire to have equitable trades between sites: I send you 1,000 visitors, you send me 1,000 visitors in return. Thus, there is no disparity in the traffic flow between larger and smaller sites.

Appendix E

Overview of Internet Filtering Software

Taken from the Electronic Network Consortium
23F, Mita Kokusai Bldg., 1-4-28 Mita, Minato-ku, Tokyo 108-0073, Japan

Overview

Software developers have responded to concerns about protecting children from objectionable content on the Internet by developing "filtering software" to enable parents and other supervising adults to set content and access preferences for children. Most filters currently act simply as content filters. Software companies are now working to add privacy preferences to their content filters. In the future, label-reading software could enable consumers to set their computers to access only those Internet sites whose privacy policies match their privacy preferences.

Content screening software uses either a filtering or rating method. The filtering method allows access to the Internet, but blocks the sites (or materials) that the software publisher defines as objectionable. Typically, the software recognizes a database of banned sites and search words. The database, however, requires regular updating, which may be at a cost to users through subscriptions. This design is not foolproof. It does not prevent a user from clicking on a link to a site that is not in the database, and it cannot stop a clever search that avoids the search words listed in the database.

The rating method blocks access to sites that do not bear a particular rating. The two currently operational rating systems are Recreational Software Advisory Council on the Internet (RSACi)[(1)] and SafeSurf[(2)]. Rating programs identify a site's HTML code and only those that contain the code with the rating are allowed through. Parents can, for example, restrict their children's access to sites that are rated as having no sexual material, foul language, or violence. This rating method uses the Platform for Internet Content Selection (PICS) specifications described in Section II of this Workshop report. SafeSurf and RSACi use the PICS format, but rely on Web sites to rate their own pages, while they reserve the right to verify each site's rating. Only a minority of existing Web sites is currently rated by these systems. Filtering software companies can add additional blocked sites to their databases on an ongoing basis. Rating systems, however, are largely relying on Web sites to insert rating labels on their sites, and sites have been slow to do so.

The explosive growth of the Internet makes it very difficult for software programs to completely monitor and control access to Internet sites. By the time a list of blocked sites is installed, thousands of new sites may have appeared. Moreover, since only a small percentage of existing sites has been reviewed, unreviewed Web sites are screened using search or trigger words or phrases. Objectionable

sites, however, can still slip through the filters. For example, a new site may have a Web address that appears to be innocuous, but may in fact contain objectionable content. Until it is manually screened, it may not be filtered out. In addition, a site may contain explicit graphics alongside unrelated text, which cannot be detected even by software that filters full text as it appears on the screen. Foreign languages and unusual spellings may also bypass filter software. Conversely, unintentional blocking may occur, preventing access to harmless medical and historical data. Phrases with dual meanings or contexts can also cause unintentional blocking. For example, a site containing Hitler's name or the word "fascism" may be blocked because the filter screens for hate content. To some extent, if the software can be customized, some of these problems can be alleviated by allowing the supervising adult to adjust the software's lists.

The various filtering software products offer a wide range of features. The least complicated software simply maintains a list of Web site addresses and blocks user access to the sites on the list. Some products offer the option of using lists and employing PICS compliant rating systems as a backup filter. Many programs offer a monitoring option, which creates a record of where the user attempted to go and when. This can be either in addition to or as an alternative to blocking access. Programs may also shut down an application entirely or e-mail the "Administrator"[3] of an attempt to access a blocked site. Filtering can vary as well, from one-way, where only the incoming text is screened, or two-way, where what the user types in (ie., a computerized order form or e-mail) is also monitored. Two-way screening is useful to prevent the flow of personally identifiable information. Two-way screening occurs in conjunction with custom lists of blocked terms, including names, addresses, birth dates, and credit card numbers. Currently only four products, Cyber Patrol, Cybersitter, Net Nanny, and Specs for Kids, are able to prevent a child from sending out the blocked information. While some products are limited to interactions on the Internet, many give users the option to continue screening offline, in word processors, games, financial managers, and any other software on the computer.

Server-based filtering options, available more commonly for business use, install filters directly on the server of a system of computers (usually a Local Access Network). This option serves all computers directly attached to the network, as well as those connecting through a dial-up service by modem. Most filtering packages created for home use, however, are client-based, meaning software is installed directly by the user and is limited to their system, regardless of their mode of online connection (modem, LAN, etc.). While the difficulty of setup varies, all software packages are fairly simple. The actual installation, whether the software is downloaded from the Internet to the hard drive or by floppy disk, occurs in a matter of minutes. Configuration is more complicated, and the time needed is directly related to the complexity of the software. Those which offer customizable lists, multi-user options, PICS compliant lists, and other choices take longer to set up and master. Most instructions are clear, and technical support is readily available with each package, making it possible to get any

software package up and running in a short period of time. Though prices vary, many home and school editions are available for free or at a low cost. Many server-based online services provide filtering software at no additional cost to their members.

Major Online Services

Each of the major online providers is increasing its efforts to create a safer environment for children using the Internet. America Online (AOL) offers parents a number of blocking options. Parents may limit their children's access to the "Kids Only" or the "Teens Only" areas, which consist of preselected entertainment and educational sites, as well as adult monitored chat and message areas. Users are kicked out of a chat room if the supervisor deems their language to be inappropriate. AOL's Member Profile, e-mail, and chat areas permit extensive collection of personal information. A parent may block a child from all chat rooms and Internet newsgroups on AOL. The option of presetting billing limits is also provided. AOL offers its members Cyber Patrol, which is described below.

Prodigy provides parents with the option to control access to its individual bulletin boards, chat areas, or newsgroups. Parents can also block complete access to the Web for certain users. Prodigy offers kids and teen chat rooms, as well as special Web areas exclusively for children and teens. Prodigy also makes Cyber Patrol available to its members. Within Prodigy's chat rooms and public forums, users are prevented from posting items deemed unacceptable for children.

CompuServe offers parents the option of controlling which areas members of the family can enter by using passwords. No chat areas are available for children. Parents have the option of having e-mail sent to them first for screening before a child receives it. CompuServe also makes Cyber Patrol available to its members.

Microsoft's new browser, Internet Explorer 3.0, offers a built-in parental control feature. Through the "Ratings" options menu, the Administrator can select to block access to a site or single page based on a number of content categories, e.g. violence, nudity, and adult language. The default parental controls are based on the RSACi standards, but the Explorer will also support ratings from any organization that follows the PICS standard.

SUMMARY OF FILTERING SOFTWARE

SurfWatch

SurfWatch, by Spyglass Inc., screens for objectionable content (violence, hate crimes, drugs/alcohol and sex) on the Web and in chat rooms. SurfWatch screens using a list of objectionable Web addresses (updated monthly) and specific trigger words within an address. Unreviewed sites and those that do not

contain the identified trigger words within their Web addresses may not be blocked. SurfWatch claims to block over 10,000 sites. SurfWatch does not work with the online services. The Administrator can independently update the SurfWatch lists or create his or her own inclusive or exclusive lists.

Cybersitter

Developed by Solid Oak Software, Cybersitter filters the Web, newsgroups, chat rooms, and e-mail and also offers the option of blocking offline applications, including games. It blocks sites related to adult themes such as sex, hate, violence, and drugs. Most importantly, Cybersitter addresses privacy issues by offering a custom blocking service, allowing a user to create a list of words and phrases that screen both incoming and outgoing information, in addition to the default restrictions. This can prevent the transfer of information such as credit card numbers and other personally identifiable information. Its "Advanced Phrase Definitions Capabilities" allows a user to offer sentence combination possibilities -- [I, we] live [at, on] [1234] [Main Street] to maximize the prevention of the transfer of such information. For additional blocking, a user can choose to add the PICS standard rating systems, which are included in the package. The program does not block sites that have not been rated by one of the lists. A unique feature of Cybersitter is its "Intelligent Phrase Filtering" system, which looks at words in context to prevent accidental access or unnecessary blocking of phrases with multiple meanings. It also offers the option of logging the sites visited without actually blocking them.

Net Nanny

Trove Investment Corporation's Net Nanny emphasizes the parents' role in determining what is appropriate for their children, rather than the software company's determination. It offers a custom dictionary that is entirely defined by the Administrator. The Administrator can control transfer of personal information and credit card numbers. The Administrator can also control access to chat areas and Web sites, as well as to any program executable on both Windows and DOS, including all online services. To provide assistance, Net Nanny has created a sample dictionary list as a start-up point. Once the list is completed, the package screens both incoming and outgoing information. It also maintains a log of blocked sites and can display the frequency of each type of violation. On request, the Administrator can choose to have the system shut down after a pre-selected number of violations has occurred.

Cyber Patrol

Cyber Patrol, a Microsystems Software Inc. product, filters objectionable material on online services, the Web, and chat rooms and continues filtering offline software programs as long as the Internet connection is maintained. It works with either an exclusive "CyberNot" list or an inclusive, but more restrictive,

"CyberYes" list. The Administrator can customize either list to include or exclude particular sites. The Administrator may also review a series of content categories and choose those that are appropriate for each user. Cyber Patrol is not able to filter new sites with unidentifiable addresses. It can filter by time of day or by total hours allowed. Upon request, the package can generate reports and charts of time usage. Cyber Patrol also addresses privacy concerns with its newly added "ChatGard." This feature enables the Administrator to block transfer of personally identifiable information using a custom list of words and phrases. When information from this list is typed in, "x" marks appear on screen instead. Cyber Patrol is now offered by AOL, CompuServe, and Microsoft's Internet Explorer. It is also PICS compatible and can read SafeSurf and RSACi ratings.

Net Shepherd

Net Shepherd, marketed by Net Shepherd Inc., enables the Administrator either to independently rate Web pages using an onscreen, point-and-click ratings bar or to screen sites using any of the PICS compliant rating systems, such as SafeSurf or RSACi. The Administrator can rate sites as "general," "child," "pre-teen," "teen," "adult" or prohibited. Net Shepherd can be configured to block unrated material or to create a list of selected sites. It is not designed to screen sites that do not bear ratings, and it only block sites on the Web and not newsgroups or chat rooms. Net Shepherd Inc. plans to extend the same rating and filtering capabilities to newsgroups.

Parental Guidance

Providence Systems markets Parental Guidance, which categorizes sites as "child," "adolescent," or "parent." Parental Guidance has approved over 100,000 sites and offers the option of downloading approximately 20,000 new sites each month. The list of approved Web sites is provided by the McKinley Group, which publishes the McKinley Internet Directory. The program also enables the Administrator to restrict access to specific newsgroups and chat areas. While Parental Guidance does not directly target the collection of personal information, the Administrator may add sites to the McKinley list that he or she feels are inappropriate. Another product, Parental Guidance Plus, permits the Administrator to block a user's access to offline programs, control the amount of time spent on the computer, and monitor its usage.

Specs for Kids

Newview, Inc.'s Specs for Kids creates an inclusive environment in which children can explore the Internet. The Specs for Kids home page includes a search tool and links to reference tools, news sources, entertainment, and other pages approved for children's access. In addition, the Administrator can customize the software to create a dictionary of restricted words and phrases to override the default inclusive list. Administrators may choose between five

different levels of restriction within 15 rating categories, including a whole range of adult topics. Specs for Kids is PICS compliant and has added such screening categories as credit cards and advertising, preventing the transfer of some personally identifiable information. One limitation of the program is that it does not prevent a child from transferring information on a site approved by Specs for Kids' reviewers. Upcoming editions plan to support blocking of individual newsgroups and chat rooms and to include an encryption capability for all messages. Specs for Kids is not compatible with the online services.

---

1. The Recreational Software Advisory Council (RSAC), an organization initially formed by software publishing companies in 1994 to rate video game software for violence, adapted its rating system to the Web and expanded the categories to include ratings for the level of violence, sex, nudity, and offensive language. The RSAC asks Web sites to create ratings for their own pages by answering a questionnaire at the RSAC's home page. After completing the questionnaire a PICS-compatible HTML tag is designated and the site can insert it into its pages. The tag is then added to the RSACi ratings system. The RSAC reserves the right to verify the accuracy of each rating. A number of the filters described in this Appendix support the RSACi ratings system, including Cyber Patrol, Microsoft Internet Explorer 3.0, Net Shepherd, and SurfWatch.

2. SafeSurf was begun by a group of parents in 1995 to create a "child safe" environment on the Internet. Its Web site provides HTML tags that Web sites can use to rate their sites according to SafeSurf's criteria.

3. This appendix uses the term "Administrator" to refer to the person who controls the implementation of the filtering software, i.e., the parent, teacher or employer who installs and configures the software program

Appendix G:
Samples of Meta-Tags and Labeling Systems

1.0 Surf Watch
Section One: Adult Themes with Caution Levels

SS~~001. Profanity

1) Subtle Innuendo
Subtly Implied through the use of Slang
2) Explicit Innuendo
Explicitly implied through the use of Slang
3) Technical Reference
Dictionary, encyclopedic, news, technical references
4) Non-Graphic-Artistic
Limited non-sexual expletives used in a artistic fashion
5) Graphic-Artistic
Non-sexual expletives used in a artistic fashion
6) Graphic
Limited use of expletives and obscene gestures
7) Detailed Graphic
Casual use of expletives and obscene gestures.
8) Explicit Vulgarity
Heavy use of vulgar language and obscene gestures. Unsupervised Chat Rooms.
9) Explicit and Crude
Saturated with crude sexual references and gestures. Unsupervised Chat Rooms.

SS~~002. Heterosexual Themes

1) Subtle Innuendo
Subtly Implied through the use of metaphor
2) Explicit Innuendo
Explicitly implied through the use of metaphor
3) Technical Reference
Dictionary, encyclopedic, news, medical references
4) Non-Graphic-Artistic
Limited metaphoric descriptions used in an artistic fashion
5) Graphic-Artistic
Metaphoric descriptions used in an artistic fashion
6) Graphic
Descriptions of intimate sexual acts
7) Detailed Graphic
Descriptions of intimate details of sexual acts
8) Explicitly Graphic or Inviting Participation
Explicit Descriptions of intimate details of sexual acts designed to arouse. Inviting interactive sexual participation. Unsupervised Sexual Chat Rooms or Newsgroups.
9) Explicit and Crude or Explicitly Inviting Participation
Profane Graphic Descriptions of intimate details of sexual acts designed to arouse. Inviting interactive sexual participation. Unsupervised Sexual Chat Rooms or Newsgroups.

SS~~003. Homosexual Themes

1) Subtle Innuendo
Subtly Implied through the use of metaphor
2) Explicit Innuendo
Explicitly implied (not described) through the use of metaphor
3) Technical Reference
Dictionary, encyclopedic, news, medical references
4) Non-Graphic-Artistic
Limited metaphoric descriptions used in an artistic fashion
5) Graphic-Artistic
Metaphoric descriptions used in an artistic fashion
6) Graphic
Descriptions of intimate sexual acts
7) Detailed Graphic
Descriptions of intimate details of sexual acts
8) Explicitly Graphic or Inviting Participation
Explicit descriptions of intimate details of sexual acts designed to arouse. Inviting interactive sexual participation. Unsupervised Sexual Chat Rooms or Newsgroups.
9) Explicit and Crude or Explicitly Inviting Participation
Profane Graphic Descriptions of intimate details of sexual acts designed to arouse. Inviting interactive sexual participation. Unsupervised Sexual Chat Rooms or Newsgroups.

Appendix H:
List of Banned Meta-Tag Terms
Adult Sites Against Child Pornography

- 4teen
- 6teen
- 7teen
- adolescent
- child
- child porn
- child pornography
- child sex
- childporn
- children
- childsex
- forteen
- illegal lolitas
- juvenile
- kid porn
- kiddie
- kiddie porn
- kiddie sex
- kiddieporn
- kiddiesex
- kinderporn
- kindersex
- koprofgie
- kotoran
- lolita
- lolitas
- lolitaz
- minor
- minors
- paedophilia
- paidophilia
- pdophile
- pdophilie
- pederastia
- pediphile
- pedofilia sex
- pedoland
- pedophelia
- pedophile
- pedophilia
- pedophilia pictures
- pedophylia
- pre teen
- pre teenage
- pre teenager
- pre teenagers
- pre teens
- pre-adolescent
- preeteen
- prelolitas
- pre-teen
- pre-teen porn
- pre-teen sex
- sex with children
- sex with minors
- sixteen
- teen 13
- teen 14
- teen 15
- teen 16
- teen 17
- teen13-17
- under age
- underage
- underaged

Appendix H:
List of Banned Meta-Tag Terms
Adult Sites Against Child Pornography

- 4teen
- 6teen
- 7teen
- adolescent
- child
- child porn
- child pornography
- child sex
- childporn
- children
- childsex
- forteen
- illegal lolitas
- juvenile
- kid porn
- kiddie
- kiddie porn
- kiddie sex
- kiddieporn
- kiddiesex
- kinderporn
- kindersex
- koprofgie
- kotoran
- lolita
- lolitas
- lolitaz
- minor
- minors
- paedophilia
- paidophilia
- pdophile
- pdophilie
- pederastia
- pediphile
- pedofilia sex
- pedoland
- pedophelia
- pedophile
- pedophilia
- pedophilia pictures
- pedophylia
- pre teen
- pre teenage
- pre teenager
- pre teenagers
- pre teens
- pre-adolescent
- preeteen
- prelolitas
- pre-teen
- pre-teen porn
- pre-teen sex
- sex with children
- sex with minors
- sixteen
- teen 13
- teen 14
- teen 15
- teen 16
- teen 17
- teen13-17
- under age
- underage
- underaged