Hacktivism and Habermas:

Online Protest as Neo-Habermasian Counterpublicity

A thesis submitted in partial fulfilment of the

requirements for the Degree

of Doctor of Philosophy in Media and Communication

in the University of Canterbury

by Tessa Jade Houghton

University of Canterbury

2010

Table of Contents

List of Tables and Figures

Acknowledgements

Thank you.

First and foremost, Sally and Keith Houghton. For having always supported me, encouraged me, and provided me with opportunities, even when I didn't deserve them. I feel privileged to have such amazing parents.

To those friends who know what true friendship and support is, who have provided both honestly and unconditionally, and who have inspired me to keep on going. You have my respect and loyalty always.

To my supervisors, Dr. Mohammed Musa and Dr. Linda-Jean Kenix, for the guidance, understanding and encouragement given throughout the writing of this thesis.

To the Department of Media and Communication at the University of Canterbury and to the University as a whole, for awarding me a scholarship, and for providing employment and development opportunities, as well as conference funding. I am immensely grateful for this financial support.

fall down seven times,
get up eight

Abstract

This thesis both draws from and contributes to the ongoing project of critiquing and reconstructing the theory of the public sphere; an undertaking that has been characterised as both valuable and necessary by Fraser (2005: 2) and many others. The subsection of theory variously described as 'postmodern', 'radical', or 'agonistic' informs an intensive practical and theoretical critique of the pre- and post-'linguistic turn' iterations of the Habermasian ideal, before culminating in the articulation of a concise and operationalisable 'neo-Habermasian' public sphere ideal. This revised model retains the Habermasian public sphere as its core, but expands and sensitizes it, moving away from normative preoccupations with decision-making in order to effectively comprehend issues of power and difference, and to allow publicness "to navigate through wider and wilder territory" (Ryan, 1992: 286).

This theoretical framework is then mobilised through a critical discourse analytical approach, exploring three cases of hacktivist counterpublicity, and revealing the emergence of a multivalent, multimodal discourse genre capable of threatening and fracturing hegemony. The case studies are selected using Samuel's (2004) taxonomy of hacktivism, and explore the 'political coding' group, Hacktivismo; the Creative Freedom Foundation and the 'performative hacktivism' of their New Zealand Internet Blackout; and the 'political cracking' operations carried out by Anonymous in protest against the Australian government's proposed Internet filter.

The analysis focuses on how the discursive form and content of hacktivism combines to function counterhegemonically; that is, how hacktivists work to provoke widespread political preference reflection and fracture the hegemony of the publics they are oriented against. This approach generates a fruitful feedback loop between theory and empirical data, in that it enriches and extends our understanding of new modes of counterpublicity, as well as providing a detailed account of the under-researched yet increasingly widespread phenomenon of hacktivism.

Chapter 1

Introduction

> …the public sphere theory is in principle an important critical-conceptual response that should be reconstructed rather than jettisoned, if possible.
>
> (Fraser 2005: 2)

The fulcrum upon which this thesis rests is the Habermasian concept of the public sphere, as elucidated in *The Structural Transformation of the Public Sphere* and in Habermas's later, 'post-linguistic turn' iterations. Some version of the public sphere has always been linked to democracy (Dahlgren 1991: 1), but since its translation into English in 1989, this seminal text and Habermas's subsequent reconfigurations of its central concept have provoked much critical attention, with the enduring popularity of the concept in its various forms testament to its fundamental theoretical power and utility.

The central importance of the concept of the public sphere is that it allows us to generate ideal conditions for and boundaries to the kind of deliberation regarded as democratically legitimate. It is of central importance to the wider field of deliberative democratic theory, which seeks to transform the democratic process from one that merely aggregates individual preferences, into one that transforms these preferences through processes of deliberation and debate. It asserts that political communication cannot serve democracy unless it is deliberative and occurs amongst an inclusive and heterogeneous group of participants (Witschge 2004: 110). This envisaged state of affairs has become commonly understood as 'strong democracy' (Barber 1984), and advocates the recurring participation of all people in activities of self-governance, urging "that we take ourselves seriously as citizens" (Barber 1984: xvii). It seeks to collectively relocate power downwards, rendering

governments less susceptible to distortion or domination by social or economic elites.

However, as Fraser notes in the quote above, and as has been echoed by countless others (see: Calhoun 1992; Dahlgren 1991: Kellner 2000), the very significance of the public sphere theory demands that we do not rest on our laurels and uncritically accept its status and definition as fixed, by deferring only to Habermas's articulations (inarguably sophisticated though they are). As with almost any theory, it should not be viewed as a static achievement, but an ongoing project of refinement and reformulation. Indeed, coming to some kind of final and enduring consensus on how we should conceive of public sphere theory is an impossible task (much as achieving any kind of rational consensus is a similarly impossible task, as is argued within) – the inherent social embeddedness of the concept necessitates constant revision and re-articulation in order that it may keep pace with fluidity and dynamism of society (Dahlgren 1991: 3).

This thesis is intended as a contribution to this ongoing project. It seeks to build upon the thread of public sphere criticism and reformulation variously described as postmodern, post-structuralist, radical, or agonistic, through synthesizing the manifold perspectives this thread contains into a concise and operationalisable theoretical iteration, dubbed neo-Habermasian public sphere theory. This theoretical synthesis project retains the Habermasian public sphere as its core, but expands and sensitizes it in keeping with Fraser's influential criticisms (1992), moving away from normative preoccupations with decision-making in order to more effectively comprehend issues of power and difference, and to allow publicness "to navigate through wider and wilder territory" (Ryan 1992: 286). This breaking of new theoretical territory requires, amongst several other redevelopments, that the Habermasian requirements of the ideal speech situation be relaxed, thus allowing contestatory forms of communication such as non-coercive activism into the global network of public and counterpublic spheres.

This theory is then applied in the interpretation of hacktivism, or online direct action. This is a phenomenon that emerged during the nineties, and although it has received some notable academic attention, its investigation through a public sphere theoretical lens is sorely lacking. Broader interpretations of its democratic

significance have been made, but the intersection of actually occurring hacktivism and the public sphere theory generates fruitful new understandings and directions for both fields, providing a focused perspective on hacktivism that counters the negative associations it is so often tarred with due to its hacker ancestry, as well as necessitating extension and innovation within the theory of the public sphere.

1.1 An overview of the thesis chapters

Chapter 2 provides and overview of the methodological journey and choices informing the research, beginning with a reflection on the difficulties encountered in researching hacktivism. It presents a rationale for the change in methodological approach from quantitative to qualitative, and the decision to utilise critical discourse analysis (CDA). It gives an overview of the strengths and weaknesses of the CDA approach, and outlines the key CDA theories and texts used to construct the particular focus and framework applied within the thesis. The theoretical framework or tripartite hacktivist typology proposed by Samuel (2003) is introduced and applied in the selection of three thesis case studies. The case studies and the data corpus associated with each of them are briefly identified. Finally, the two core research questions for the thesis are defined.

Chapter 3 comprises the first half of the literature review on hacking and hacktivism. It introduces the concept of hacking and the evolutionary progression of computer hacking, and outlines the seven generations of computer hacker outlined in the academic literature, from the early or 'true' hackers experimenting with and innovating on early mainframe computers, through the corporatised and criminalized iterations of the practice, to the resurgence of 'hacking for a cause' embodied by the free and open source software movement (FLOSS) and hacktivism. The core tenets of an enduring 'hacker ethic' are elucidated, as is the polysemic and contested nature of 'the hack' and the media's ongoing characterisation of all hackers as 'electronic bogeymen'. Primary material from interviews with New Zealand hackers is used to ground the secondary research

summarised in both this chapter and the conclusion to the literature review provided in the following chapter.

Chapter 4 concludes the literature review with a detailed summary of the significant existing literature on hacktivism, and extends upon the introduction to the practice provided in the previous chapter. From the theoretical hacktivism proposed and anticipated in early literature, to the actual materialisation of the practice in the early nineties, this chapter explores the emergence and variety of this new form of digital direct action or protest. It summarises hacktivism's inheritance of the media-fuelled image problems associated with hacking, and situates the practice within a broader 'repertoire of electronic contention'. It assesses various attempts at generating an internal typology of hacktivism before identifying the most successful of these attempts, and concludes with an identification of the need for hacktivism to be explored through a public sphere theoretical lens.

Chapter 5 introduces this theoretical lens by starting with what is commonly regarded as the central textual hub of public sphere theory – Jürgen Habermas's *The Structural Transformation of the Public Sphere*. It summarises this seminal text's tracking of the rise, transformation and decline of the historically specific Westphalian-national bourgeois public sphere in England, France and Germany. The contradictory exclusions inherent to these partially realised public spheres are explored, as is the subsequent refeudalisation of society and the public sphere, with particular attention paid to the role of the mass media in this process. The chapter concludes with a concise summary of Habermas's 'post-linguistic turn' work on public sphere theory, with particular attention paid to the concepts of and tension between the 'lifeworld' and 'system', and his theory of communicative legitimacy and articulation of the procedural constraints of the 'ideal speech situation'.

Chapter 6 extends from this theoretical hub, beginning with an exploration of the historical inaccuracies or practical criticisms of the Habermasian public sphere as elucidated in *Structural Transformation*; specifically, Habermas's overidealisation of the internal function of the bourgeois public sphere; his lack of acknowledgement of the existence of multiple historical public spheres and of class- and gender-based exclusions inherent in the bourgeois public sphere; and his over-pessimistic analysis of the contemporary media and public sphere. Nancy Fraser's renowned theoretical

criticism of the Habermasian public sphere (1992) is first summarised, with its central critical tenets then providing a framework for an extended exploration of the wider universe of theoretical criticisms stemming from what has been variously described as a postmodern, poststructuralist, radical, or agonistic theoretical perspective on deliberative democracy and the public sphere. These criticisms focus on: the theorization of multiple public spheres, particularly the transnationalisation of the concept and the idea of counterpublic spheres; the erosion of the theoretical barrier between public and private, particularly the impossibility of bracketing status differentials and the failure of rational-critical debate; the democratic advantages in allowing private interests into the public sphere; and the failures of the concept of rational consensus. The chapter concludes with the synthesis of this body of criticisms into a new normative public sphere ideal, postulating a 'neo-Habermasian' view of the public sphere that more adequately accounts for issues of power and difference, and answering the first research question of the thesis.

Chapter 7 brings together the two threads established in chapters 3 to 6 through summarising the literature of hacktivism and assessing the resulting definition of hacktivism through the neo-Habermasian theoretical lens established in the previous chapter. This assessment established that hacktivism is, by its very definition, a legitimate form of neo-Habermasian public sphere communication, in that it induces political preference reflection in a disruptive but non-violent and non-coercive fashion (as does any other form of non-violent activism). The chapter serves to introduce the second research question of the thesis, which is addressed within the subsequent three chapters and their focus on the three hacktivist case studies introduced in Chapter 2.

Chapter 8 explores the case of Hacktivismo, a multi-national group of 'political coders' (Samuel 2003). It begins with an introduction to the group and their early activities, before briefly outlining the central utility of each of the 'political coding' projects or political software programmes they have been involved in creating. A broad discourse analysis of the textual artifacts available on their website and in other locations is conducted, thus establishing the central collective ideology or purpose of their hacktivist counterpublicity. The chapter also introduces the

'Hacktivismo Declaration' – the group's central ideological text or code of practice, which comprises the central text subjected to a close critical discourse analysis later on in the chapter. This close analysis is preceded by an identification of the 'constellation of publics' Hacktivismo exists in relation to; that is; the dominant or pseudopublics they are opposed to and the publics or counterpublics that comprise their audience. The analysis itself focuses on the self-presentation and negative-other presentation encoded in the Declaration, before concluding with an analysis of the way in which the group's textually articulated 'intellectual ideology' (Billig et al 1988) is launched into wider circulation through their software project, and how this and the projects themselves effect political preference reflection and attempt to destabilise the dominant publics Hacktivismo is engaged in counterpublicity against.

Chapter 9 focuses on the New Zealand Internet Blackout led by the Creative Freedom Foundation (CFF), a group of New Zealand-based 'artist-activists (Samuel 2003). The Blackout was mobilised against proposed amendments to New Zealand copyright legislation that would have rendered it "arguably the world's harshest copyright enforcement law" (Saarinen 2009). A broad discourse analysis of the CFF's website is used to establish their intellectual ideology and the ways the website and its attendant web technologies operate in aid of the dissemination of this ideology. The chapter then gives an account of the Blackout as an episode of performative hacktivism (Samuel 2003), before the CFF's constellation of publics is articulated. The central Blackout text is then subjected to a close discourse analysis, and the Blackout itself interpreted in terms of its subversion of the usual channels of access to publicity, and the way in which it generated a viral flow of counterpublicity that provoked widespread political preference reflection and destabilised the dominant or pseudopublics the CFF run counter to.

Chapter 10 rounds out the trio of case studies with an account of the 'political cracking' (Samuel 2003) campaign carried out by the internet-based hacktivist/prankster collective known as Anonymous, against the Kevin Rudd-led Australian Labor government, and their proposed national internet filter. It begins with an introduction to the collective and their various activities, before exploring wider opposition to the planned censorship. The two hacktivist 'Operations'

mobilised by Anonymous are detailed, and the central text articulating the collective's intellectual ideology and other informative textual artifacts are analysed in order to then identify Anonymous's constellation of publics. The chapter then surveys the way in which Anonymous's Operations both launched their textually articulated counterpublicity into broader circulation and constituted an inherent critique of the filtering plan in and of themselves, in order to provoke political preference reflection and destabilise the dominant or pseudopublics they were opposed to.

The thesis is concluded in Chapter 11, which summarises the major contributions of the thesis, and what has been discovered with relation to the two research questions. It begins with a summary of the findings drawn from the case studies with regards to the second empirical research question, before contextualising these findings in light of neo-Habermasian public sphere theory and the first theoretical research question. It provides suggestions for those engaging in further research on the subject, and argues for both the ongoing importance of the concept of the public sphere, and the need for public sphere theory to keep pace with the ongoing dynamics of societal and communicative change.

Chapter 2

Methodology and research questions

> There are no right or wrong methods. There are only methods that are appropriate to your research topic and the model with which you are working.
>
> (Silverman 2010: 124)

Hacktivism is a relatively new topic of research, and neo-Habermasian public sphere theory, although built upon an extensive historical theoretical background, is a new theoretical concept. Needless to say, the intersection of the two does not have any well-beaten path to follow. As such, this thesis is more of an exploratory journey than a re-examination or slight departure from an established theoretical and methodological tradition within a particular topic of research. This journey has had its challenges and setbacks, and while these have been frustrating, they have been mistakes that have facilitated greater learning. Indeed, I believe that the process of working past these difficulties has been one of the most personally fruitful aspects of this research. As such, this methodology chapter is loosely based on the 'natural history' form suggested by Silverman (2010). Rather than being strictly impersonal and passively voiced, it will offer what Silverman, borrowing a phrase from Alasuutari, calls "fieldnotes about the development of one's thinking" (1995: 192, in Silverman 2010). This approach does not attempt to substitute style for substance – the key methodological questions are still answered – but it grants the reader access to the research thought process and the degree of self-criticality of the researcher.

The rationale behind this approach is twofold. Firstly, "a highly formal chapter can be dull to read as well as dull to write" (Silverman, 2010: 334). It is hoped that this thesis provides an interesting and even enjoyable read, as well an informative one, and a methodological chapter in continuation rather than in contrast with this goal is surely preferable. Secondly, "'methodology' has a more flexible meaning in

qualitative research than in its quantitative sister" (ibid.: 334). In qualitative research, a methodology refers to "the choices we make about cases to study, methods of data gathering, forms of data analysis etc. in planning and executing a research study. So our methodology defines how one will go about studying any phenomenon" (ibid: 110). A more richly descriptive, active explanation of these choices thus makes more sense than a "series of blunt assertions in the passive voice" (ibid.: 334). Thirdly, a thesis is intended to show research competence. Hence, it is appropriate to include some kind of historical component to the methodology, including "difficulties and dead ends" (ibid.: 335).

2.1 Finding an appropriate methodology: False starts and dead ends

This research stemmed from what can best be described as enthusiastic and interested but rather vague beginnings. I did not encounter either the concept of hacktivism or the public sphere until the Honours year of my undergraduate degree, but in that same year, quickly became fascinated by the wider field of media political economy within which public sphere theory is situated, and by the general debate over the democratic potential of the Internet. The limited amount of reading I had done on the theory of the public sphere and on Internet activism in general and hacktivism in particular, suggested that there was both fresh research ground to be broken in this intersection of theory and subject.

I thus began my research with the intent of assessing whether hacktivism fulfilled the Habermasian ideal of the public sphere, as outlined in *The Structural Transformation of the Public Sphere* and later post-linguistic turn Habermasian texts. My original methodological plan was to procure a sample of recorded hacktivist actions and websites that was representative (that is, provided a typical subsection) of hacktivism as a whole, and perform a content analysis in order to assess the extent to which they met Habermas's criteria of democratic communicative legitimacy. This content analysis was to be combined with responses from hackers/hacktivists to a survey designed to gauge their beliefs

regarding hacktivism and tease out any opinions relevant to hacktivism as counterpublic activity, and with follow-up interviews and personal communication with amenable parties. The initial plan, therefore, was to use content analysis to generate the primary data for this research, and supplement it with findings from a survey and interviews.

2.1.1 Difficult subjects, and the inappropriateness of quantitative methods

However, the more I learnt about hacktivism, the more I realised that my plan to conduct a content analysis on a representative sample of hacktivist texts was unfeasible. Hacktivism itself is extremely diverse, and the records of hacktivist events and groups even more so. Not all hacktivist groups have websites upon which they detail their intentions and political opinions, there is no 'directory of hacktivism', or central population record from which to take a sample, and hacktivism utilises a variety of tools and approaches, the permanent records of which (if they exist) vary widely, therefore there would be insufficient comparability between the texts analysed.

Furthermore, the pilot survey I distributed to hackers asking them about their own activities, about any hacktivism they might have been involved with, and about their thoughts on hacktivism in general, met with abortive results. I distributed this survey, which included both quantitative and qualitative elements, at the first ever New Zealand hacker's conference, Kiwicon, at the end of 2007. I was lucky that this conference occurred when it did (and has continued to occur), in that it gave me first hand experience of and with a subsection of the hacker community, which is a rare experience for an 'outsider', given that hackers do not often come together in such numbers, and indeed, had not previously done so in New Zealand. This provided me with an important chance to ground my increasing understanding of the diversity of hacking, and of the inaccuracies in the media portrayal of the activity. Seeing hackers and/or computer security professionals present their work,

simply observing them interacting with one another, and acquiring a first-hand experience of the actuality of the community rather than simply reading about it in the abstract was a valuable experience for me. As one of the organisers of the event put it (in a personal communication stemming from my attendance of the conference, further details of which will be discussed shortly):

> I would think Kiwicon would be a pretty unique opportunity for people interested in observing hackers in their natural environment – there's never been an event on the scale of Kiwicon before in New Zealand.
>
> (Metlstorm 2007)

Given the short duration of the conference (2 days), I would not go so far as to make any structured ethnographic claims regarding the research value of the experience, but it certainly brought my research topic out of the abstract and into a concrete focus, and corroborated some of the information gleaned through the literature review.

However, although I spoke to several hackers at and after the conference, only one of them hinted at having any involvement with hacktivism (and politely declined to talk about it, citing (justifiable) 'paranoia', although was happy to discuss it with me in the abstract). Furthermore, I received only five survey returns out of around 200 conference attendees, despite distributing the survey in person at the conference, and through the conference's mailing list. I had expected a poor response rate, but not quite that poor. As one of the attendees spoken to (the CEO of a computer security corporation) suggested, the increasing refinement and harshness of New Zealand cybercrime laws (and indeed, international laws) does not provide a comfortable environment for the relaying of one's sometimes illegal exploits to some random and unknown researcher, even one offering contractually defined anonymous and pseudonymous communication:

> I can't support, condone nor have nor would be involved in activity that goes against government cybercrime laws/acts and "good behaviour".

> A few years ago, you probably would have had people open to talking quietly about their exploits (it was more of a game then) but time has moved on and anyone involved in this activity in the US, Australia and New Zealand etc for example would be/is just plain dumb – the laws are pretty well defined now and people are being jailed.
>
> (Drazic 2007)

My literature review on hacking and hacktivism corroborates the difficulty of making contact with hackers and hacktivists – the majority of literature on the subjects deals with media representations and legal interpretations of them and their activities, but there are very few authors who have actually gained personal communicative access to computer hackers (in the illicit sense of the word), or to a wide range of hacktivists.

It was thus obvious that a survey was not an appropriate tool with which to gather research data. However, the five respondents I did acquire were all willing to speak to me using their real names or a 'handle' that could easily be traced back to their 'real life' identity, and to be questioned further about hacking and hacktivism in general. As such, I utilised the limited contact made, and either spoke to in person or communicated via email with each of the respondents, obtaining answers to some of the qualitative components of the survey and added statements they wished to make. These interviews and personal communications were not, ultimately, used to answer the research questions posed *per se*, but they did provide useful material on the concepts and history of hacking and hacktivism, which provide the essential background for this research, and their statements and my observations at the conference have thus been used to ground some of the literature reviewed.

Moreover, I no longer believed a content analysis (even if I had been able to conduct one) would yield any rich or meaningful results. Having derived a definition for and understanding of both hacktivism and the neo-Habermasian public sphere, my research question shifted from a 'how much?' form into 'how?' I was no longer exploring to what extent (or 'how much') hacktivism was a legitimate public sphere activity, but rather, how hacktivism works to generate neo-Habermasian counterpublics aimed at fracturing hegemony. This kind of constructivist 'how?' research question is clearly more suitably approached using a

qualitative methodology (Silverman 2010: 118), and by focusing on a few specific cases of hacktivism, and exploring them in detail, with the idea being to develop as full an understanding of those cases as possible within the parameters of the research question (Punch 1998: 150).

2.2 A qualitative methodology

> Any good researcher knows that your choice of method should not be predetermined. Rather you should choose a method that is appropriate to what you are trying to find out… This suggests a purely pragmatic argument ('horses for courses'), according to which our research problem defines the most appropriate method.
>
> (Silverman 2010: 10)

Having ascertained that a qualitative methodology based on analysing an appropriate yet manageable number of case studies would be most appropriate, the methodological questions then became:

1. Which cases of hacktivism should be selected, so as to best:
   a. Provide a representative sample of the diverse range of hacktivist activities, but also;
   b. Remain focused enough to ensure some element of cohesion within the sample;
   c. Provide a corpus of data for analysis?
2. How should this data be analysed in aid of answering the research question?

2.2.1 Constructing a 'data pool' of possible cases for analysis

Constructing a 'data pool' of potential cases of hacktivism for analysis poses two related problems. Firstly, unless you are directly affected by hacktivism or have access to hacktivists, you must rely on media coverage of such incidents to alert you to their presence. Secondly, once you do become alerted to a hacktivist incident, the incident may be over before you have the chance to view it 'in the wild', and you must therefore rely on others, generally either mainstream or alternative/niche media, to provide the traces of the activity, in the form of accounts and screenshots. Given the previously discussed difficulty in gaining access to most hacktivists, there was no way to avoid this reliance on secondary information. Although this would be crippling to some research, given the focus of this research, it is actually rather appropriate. As much hacktivism relies on the media to amplify its initial publicity, utilising this media publicity in terms of both data selection and collection provides a snapshot of the external or public orientation of hacktivist incidents, which is what this thesis explores. That is, although both an emphasis on public orientation and on internal dynamics fall within the wider or holistic public sphere perspective, the emphasis within this research is on the external as opposed to internal dynamics of hacktivist counterpublics.

Given this fact, and my lack of access to hacktivists themselves, I instead used the data on hacktivism that I did have access to – that is, I used external accounts of hacktivism to build my knowledge of a pool of possible cases. I constantly monitored and also did historical searches of news media, both mainstream and niche/alternative, and thus gained awareness of a wide range of hacktivist incidents and groups, both current and historical. This searching and monitoring was supplemented by the hacktivist groups and incidents mentioned in the literature I reviewed on hacking and hacktivism.

That is not to say that there are no biases with this method of identifying possible cases for analysis. Due to my monolinguality, it preselects towards hacktivism done by English speaking hacktivists in English speaking nations, and given my Australasian location, also skews towards hacktivism occurring in the same

geographical region. These would be an issue no matter what my research topic was, but it is best to acknowledge rather than occlude such a limitation, given that hacktivism is an inherently global phenomenon. Of more serious concern is the fact that relying on media reportage and previous literature for awareness of hacktivist activity preselects towards the most 'successful' hacktivist incidents and groups – i.e. the ones that have garnered the most publicity. However, given that I had no other means of access to possible cases, this was unavoidable, and given the focus of this research, this lack of access to hacktivist counterpublics with a failed or at least limited external orientation is not a severe limitation.

The problem then became one of narrowing down the material I wanted to work with, as it is obviously impossible to study each and every instance of hacktivism that one is aware of. Furthermore, "the validity of qualitative analysis depends more on the quality of the analysis than on the size of the sample" (Mitchell 1983, in Silverman 2010: 54). As such, I decided that three case studies, selected using a theoretical or purposive sampling procedure, would be sufficient, and that I would utilise a critical discourse analytical methodology in exploring them. I will discuss the selection of this sample shortly, but first present a brief rationale for the choice of critical discourse analysis as the form of analysis used, through an explanation of the fundamental characteristics of this research tradition.

2.2.2 An overview of critical discourse analysis

> Critical discourse analysis has never been and has never attempted to be or to provide one single or specific theory. Neither is one specific methodology characteristic of research in CDA. Quite the contrary, studies in CDA are multifarious. Derived from quite different theoretical backgrounds, oriented towards different data and methodologies… Hence we suggest the notion of using a 'school' for CDA, or of a programme, which many researchers find useful and to which they can relate.
>
> (Wodak & Meyer 2009: 5)

Critical discourse analysis, while not always explicitly acknowledged as such, extends from the language-based critical perspective of Western Marxism, which includes such key members and groups as Gramsci and the Frankfurt School (including Habermas) and their 'Critical Theory' (Fairclough & Wodak 1997: 261, Wodak & Meyer 2009: 6)). Like discourse analysis, it is interested in naturally occurring language; focuses on larger units of language than isolated words and sentences; looks beyond sentence grammar towards a study of action and interaction; extends to non-verbal (semiotic, multimodal, visual) aspects of interaction and communication; focuses on dynamic interactions, studies the functions of contexts of language use; and analyses a vast number of phenomena of text grammar and language use (Wodak & Meyer 2009: 2). However, in addition to this, critical discourse analysis is "by its nature interdisciplinary, combining diverse disciplinary perspectives in its own analyses" (Fairclough & Wodak 1997: 271), and it also takes a constitutive and problem oriented approach (Wodak & Meyer 2009: 2), which manifests itself in two main ways.

Firstly, CDA sees discourse (or language) as constitutive of society – as "a form of 'social practice'" (Fairclough & Wodak 1997: 258) and thus probes texts and discourse practices in order to discover "hidden meanings and value structures" (Jaworski & Coupland 1999: 33). It rejects the merely descriptive tradition of some discourse analysis, and instead is concerned with discourse as being responsible for the social construction of reality, and with the construction of ideology in particular (ibid.: 34). Ideologies are inherently associated with power relations, exclusions and inequality; hence, CDA is oriented towards a forensic examination of the construction and maintenance of ideologies, as well as resistance to these ideologies.

It assumes a dialectical or two-way relationship between discourse and social structures – "discourse is socially *constitutive* as well as socially shaped… It is constitutive both in the sense that it helps to sustain and reproduce the status quo, and in the sense that it contributes to transforming it" (Fairclough & Wodak 1997: 258). Discursive practices can both help generate and reify ideological effects or hegemony, as well as constitute resistance to these societal power stratifications. "Both the ideological loading of particular ways of using language and the relations

of power which underlie them are often unclear to people. CDA aims to make more visible these opaque aspects of discourse." (ibid.).

As such, it is sensitive to ongoing struggles for ideological dominance and resistance, and has a central concern with ideology and power. It generally understands power in the Foucauldian sense, as "a systemic and constitutive element/characteristic of society" (Wodak & Meyer 2009: 9), because it sees text as a manifestation of social action that is determined by social structure. It also concerns itself with competing discourses in public spaces, with an understanding that "[p]ower does not necessarily derive from language, but language can be used to challenge power, to subvert it, to alter distributions of power in the short and long term." (ibid.). CDA is also increasingly interested in and accepting of multimodality:

> Critical discourse analysis has moved beyond language, taking on board that discourses are multimodally realised, not only through text and talk, but also through other modes of communication such as images… Overall, then, critical discourse analysis has moved towards more explicit dialogue between social theory and proactive, richer contextualisation, greater interdisciplinary and greater attention to the multimodality of discourse.
>
> (van Leeuwen 2006: 292, in Wodak & Meyer 2009: 16)

Furthermore, as previously mentioned, the critical orientation, and thus CDA, is "not merely 'deconstructive'; it may aim to be 'reconstructive', reconstructing social arrangements" (Jaworski & Coupland 1999: 35). Rather than attempting to maintain an objective and dispassionate stance, critical discourse analysts generally take a political stance – they "see themselves as politically engaged, working alongside disenfranchised social groups" (ibid.). Indeed, social science as a whole is inherently connected to issues of politics and policy formation, and is socially embedded (Wodak & Meyer 2009: 7); CDA is simply much more explicit about this political orientation:

> What is distinctive about CDA is both that it intervenes on the side of dominated and oppressed groups and against dominating groups, and that it openly declares the emancipatory interests that motivate it… This certainly does not imply that CDA is less scholarly than other research: standards of careful, rigorous and systematic analysis apply with equal force to CDA as to other approaches.
>
> (Fairclough & Wodak 1997: 259).

Like all critical theories, it is intended to "produce and convey critical knowledge that enables human beings to emancipate themselves from forms of domination through self-reflection" (Wodak & Meyer 2009: 7).

The use of CDA is particularly appropriate in a world where language has become increasingly bound up with a range of social processes. The general shift towards service economies, and the increasingly media-saturated socio-political environment has amplified the socially constructive force and scope of discourse and language, necessitating the deployment of analytical tools capable of turning a critical perspective on this discursive universe. Indeed, CDA, as a tool of this nature, is merely an academicisation of something all citizens regularly engage in.

> A critical awareness of discursive practices and an orientation to transforming such practices as one element in social (class, feminist, anti-racist, green, etc.) struggles, - or in Gidden's terms, in the reflexive construction and reconstruction of the self – is a normal feature of everyday life. The critical analysis of discourse is therefore firstly a feature of contemporary social life, and only secondly an area of academic work. And critical discourse analysis as an academic pursuit is firmly rooted in the properties of contemporary life.
>
> (Fairclough & Wodak 1997: 260)

CDA does not, however, simply replicate this everyday critique. It draws upon specific theories and methodologies not available in everyday life, and "has resources for systematic and in-depth investigations which go beyond ordinary experience" (ibid.: 281). Indeed, it is always very strongly based in theory,

although many different theories may be operationalised or translated into, as well as explored through CDA's "instruments and methods of analysis" (Wodak & Meyer 2009: 23),

Rather than the usual (but certainly not exclusive) CDA focus on dominating or repressive discourses, the analysis undertaken here stems from the understanding that discourse or language "can be used to challenge power, to subvert it, to alter distributions of power in the short and long term." (Wodak & Meyer 2009: 10). Some within CDA have argued for more of this analytical orientation, calling it 'Positive Discourse Analysis' (PDA), in that it describes what texts 'do well' or 'get right' (Martin & Rose 2003; Martin 2004). I believe Martin is indeed correct when he supposes "it would be going too far to propose a 10 year moratorium on deconstructive CDA, in order to get some constructive PDA off the ground" (2004.: 24), and am not convinced that his dichotomisation of PDA as constructive and CDA as deconstructive is fair – deconstruction is often inherently re-constructive in and of itself. However, the focus here is certainly on what hacktivist texts and discourses attempt to 'do well' – how they attempt to challenge dominant power structures.

In terms of the analytical framework applied in the critical discourse analysis of the selected case studies, it is once more a case of creativity. Hacktivism is multi-modal in a way not generally considered by CDA, in that its multi-modality involves software, or code, as well as the usual multi-modal elements of images as well as text. It arguably constitutes a range of new discursive or speech genres (Bakhtin 1986), and hence previous discourse analyses based on specific and well-established genres and discursive forms are of little direct use. As a result, rather than following one particular trend within CDA, or focusing on one particular aspect of the text, such as transitivity, or nominalisation, as is sometimes the case, the following framework will be applied. This framework will provide the general outline for the analyses, but it will be bent and interwoven when and as necessary, in order to better comprehend what is being explored.

2.2.2.1 Context

A firm understanding of context is essential for CDA. In order to fully comprehend this, we must of course have a good grasp of the details of the case of hacktivism being analysed. This essential contextualisation will be provided by a detailed explication of each instance of hacktivism, what it is in aid of, and of the hacktivists involved in it. This will establish a format within which each case will be addressed separately, and the particular environment and background for each case study will be outlined, and will necessary involve some broad analysis of the wider discourse of the hacktivist groups involved, where this wider discourse is present.

2.2.2.2 Text

This section of the analysis of each case will be based upon a close analysis of the primary hacktivist texts constructed for and involved with each case of hacktivism. These texts vary from case to case, and will be clearly introduced and identified within the analysis itself, but they will each be closely analysed utilising a perspective borrowed from van Dijk's 'ideological discourse analysis' (a sub-category of CDA) (1995b, 1995c, 2006). This perspective understands ideologies as "organized by well-known ingroup-outgroup polarization", and expects to find such polarization to be "'coded' in talk and text" (van Dijk 2006: 126). As such, it is immensely useful for exploring the linguistic components of the texts produced by hacktivists.

There are many ways in which this general strategy can be encoded linguistically within discourse, some more relevant within hacktivism than others. The analysis here will draw on the "toolkit of analytical categories" provided by Barker and Galasinski (2001), who in turn, draw upon Halliday (1978, 1994), Halliday and Hasan (1985), and Beaugrande's (1991) discussion of Halliday's work, in combination with van Dijk's orienting perspective or focus. While any discourse

analysis is necessarily interpretive, and is "laden with researchers' attitudes and beliefs as well as the assumption that there is no ultimately 'correct' interpretation of texts (Wodak, 1999)", linguistic analysis anchored in systemic-functional linguistics goes some way towards reducing interpretive arbitrariness (Barker & Galasinski 2001: 64).

The analytical toolkit follows Halliday and Hasan's division of texts into three functional categories – the ideational, the interpersonal, and the textual (Barker & Galasinski 2001: 68). Due to our focus on hacktivism and van Dijk's focus on ingroup-outgroup polarisation, it is logical for the analysis to focus on the ideational and interpersonal elements of the hacktivist texts. The ideational function refers to texts' abilities to refer to external realities, and thus render their representation of the world intelligible. It focuses on such elements as transitivity, nominalisation, and vocabulary. The interpersonal function refers to interactions between the speaker and the addressee through the text, and focuses on such elements as mood, metalanguage, modality, and forms of address. Relevant linguistic elements within each of these two functions will be identified and interpreted, and will be accompanied by a consideration of intertextuality and non-linguistic semiotics where appropriate. This analysis will also, as and when is appropriate, utilise Goffman's concept of 'face' (1967), and the politeness theory of Brown and Levinson (1987), specifically, the concept of 'face-threatening acts'.

2.2.2.3 Access and control

Once the context and text have been established, analysed and interpreted, each case will then be explored in terms of the analytic category of discursive access and control, following van Dijk (1996). This category considers how patterns of access to and control of discourse are a major element in the enactment, reproduction and legitimation of the dominance of certain groups and institutions. However, as van Dijk states, "'access' is rather a vague notion" (ibid.: 87); hence, he outlines a more

detailed schema of discursive access, which may be applied to any given "social domain, profession, organisation, or situation" (summarised from van Dijk 2006: 87-89):

Firstly, we should consider who is in control of planning a communicative event. Planning will generally involve decisions to do with the setting (or time and place) of the communicative event, the discursive agenda, and with who is entitled (or ordered) to participate. We should also consider who is in control of the setting of a communicative event. This links back strongly to the planning component, in that the time, place, and circumstances of a given discursive events may be controlled by certain participants. These powerful or 'interaction-controlling' participants may also determine who is entitled or ordered to participate, and in what role. Differentials in distance and position, as well as differential access to 'props of power' (such as uniforms, being at the head of the table, etc.) may also obstruct equality of access.

Furthermore, we should consider who is in control of the various dimensions of speech, talk or text itself. Participants may have differential access to specified modes of communication (i.e. spoken or written), to the language being used, to the genres of discourse allowed, to various types of speech acts, and to discursive sequencing (i.e. who may take turns or interrupt). Furthermore, participants may have differential access to topics, style or rhetoric:

> "That is, virtually all levels and dimensions of text and talk may have obligatory, optional or preferential access for different participants, for example, as a function of their institutional or social power. Or rather, such power and dominance may be enacted, confirmed and reproduced by such differential patterns of access to various forms of discourse in different social situations. Thus, having access to the speech act of a command presupposes as well as enacts and confirms the social power of the speaker" (van Dijk 1996: 88)

Finally, we should consider the issues of audience scope and audience control. The power to control who may or may not listen to a particular discourse is also differential. "That is, discourse access, especially in public forms of discourse, also

and most crucially implies audience access" (van Dijk 1996: 88). The size of the audience is important, as is how successful one is at 'accessing' the minds of the audience.

These categories are (as is likely obvious) generally applied to a dominant discourse. However, as van Dijk himself states, discursive dominance is "seldom absolute; it is often gradual, and may be met by more or less resistance or counter-power by dominated groups" (ibid.: 85). As such, these analytic categories lend themselves equally well to investigating such 'counter-power', and thus provide a general outline for each case study. This analysis will again utilise the concepts of 'face', and of 'face-threatening acts' when and as relevant.

2.2.3 The use of theoretical sampling to select case studies

As previously stated, I wanted the cases analysed to provide explanations of hacktivism that were "generalisable in some way, or have a wider resonance" (Mason 1996: 6, in Silverman 2010: 139). That is, I wanted the findings within my particular cases to be able to be applied more generally (Silverman, 2010: 434). In quantitative analysis, this quality is usually obtained through the use of statistical sampling methods, which involve the selection of a random or representative sample of data from a predefined population (a sample typical of the population as a whole) using statistical criteria, with generalisations and inferences about the population in its entirety being extended from the findings within this sample (Arber 1993: 38). Generally, the larger the sample taken from within the population, the stronger the inferences that may be drawn.

This kind of large-scale and statistically guided sampling from predefined populations is not possible in most qualitative analysis, and is certainly neither possible nor appropriate for a critical discourse analysis of hacktivism. There is no predefined population whose parameters are known, and critical discourse analysis is too intensive and detailed to be applied to a large and fully representative sample

(even if one could be generated). However, generalisability in qualitative analysis can be obtained through the use of purposive and/or theoretical sampling. These kinds of sampling are often treated as synonyms, and indeed, "the only difference between the two procedures applies when the 'purpose' behind 'purposive' sampling is not theoretically defined" (Silverman 2010: 143).

As such, I used a theoretical sampling procedure to generate cases for a collective case study. Theoretical sampling generally involves selecting "groups or categories to study on the basis of their relevance to your research questions, your theoretical position ... and most importantly the explanation or account which you are developing", with this method being "designed to provide a close-up, detailed or meticulous view of particular units which may constitute ... cases which are relevant to or appear within the wider universe" (Mason 1996: 93-4, 92, in Silverman 2010: 145).

However, as my theoretical framework (neo-Habermasian public sphere theory) is not suitable for selecting a generalisable sample of cases of hacktivism, but is rather a lens through which these cases may be interpreted, I based this theoretical sampling upon Samuel's proposed taxonomy of hacktivism (2004a). This taxonomy is arguably the most sophisticated and well-supported internal categorisation of hacktivism available, and outlines three types; political cracking, performative hacktivism, and political coding. This taxonomy will be discussed in more detail within the literature review on hacktivism, but a brief description of it is merited here.

The taxonomy is constructed by the intersection of various hacktivist origins (hacker-programmer or artist-activist) and orientations (transgressive or outlaw) to generate three categories of hacktivist or hacktivism. Some potential overlap is recognised, with the origins recognised as more stable than the orientations, and the sub-characteristics of each category are more fluid still (ibid.). Transgressively oriented hacktivism "challenges the legal and political order, but still exists in relation to it and even shares some norms… such as legitimacy and accountability", whereas outlaw orientated hacktivism "completely rejects the legal and political order" (ibid.: 37). Generally (but not always), transgressive hacktivists tend to work

in medium-size groups and collaborate multinationally, whereas outlaw hacktivists tend to work solo or in small groups and collaborate nationally, multinationally and internationally. National collaborations target governments, businesses or organisations within their own country; multinational collaborators band across borders to attack a common target at the subnational, national or multinational level; and international collaboration involves hacktivists from one country targeting a government, business or organisation in another country, sometimes generating a reciprocal engagement (ibid.: 50).

Furthermore, political crackers, performative hacktivists, and political coders use different nymity practices. Political crackers use robust pseudonymity both to avoid legal consequences and declare that they are accountable to no one; political coders use weak pseudonymity to construct a digital persona that is accountable to wider Internet community, but in digital rather than physical terms, and performative hacktivists do not use pseudonyms, thus embracing their accountability to the real world (ibid.: 220). They treat anonymity as "a political tool, with different nymity choices conveying different kinds of claims about political strategy, risk, and above all, accountability" (ibid.; 222).

Table 1 (on the following page) illustrates these taxonomic variations. It is to be noted that the common forms within each category are linked to broader taxonomic differences, as they are too diverse and variable to be dealt with as structural variations in and of themselves. Furthermore, certain variations are shared by more than one of the categories of hacktivism.

Using Samuel's taxonomy as a base for the theoretical sampling of hacktivist incidents, i.e. selecting one case from each category – political cracking, performative hacktivism, and political coding – is thus the best way to ensure that the diverse nature of hacktivism is represented as fully as possible. The following variations within hacktivism will definitely be represented:

1. Origin: artist-activist or hacker-programmer;
2. Orientation: transgressive or outlaw;

And as such, further variations within hacktivism will also likely be represented in the case studies:

> 3. Nymity practices: hacktivism can be carried out by groups and individuals ranging from anonymous to pseudonymous to named;
>
> 4. Group size: individual or small to medium;
>
> 5. Collaborative scope: national to international;

VARIATIONS / TYPE OF HACKTIVISM	POLITICAL CRACKING	PERFORMATIVE HACKTIVISM	POLITICAL CODING
(1) ORIGIN	Hacker-programmer	Artist-activist	Hacker-programmer
(2) ORIENTATION	Outlaw	Transgressive	
(3) NYMITY PRACTICES	Robust pseudonymity	Use real names	Weak pseudonymity
(4) GROUP SIZE	Solo or small	Medium	
(5) COLLABORATIVE SCOPE	National, multinational or international	Multinational	
FORMS	Defacements Redirects Automated DDoS attacks Sabotage Information theft	Parodies Sit-Ins	Software development

Table 1: The variations within hacktivism represented by Samuel's (2004a) taxonomy

Choosing one case from each of Samuel's categories of hacktivism thus ensured that the three cases, when looked at collectively, provided a generalisable sample of hacktivism in general. However, I also wanted to ensure that there was some element of cohesion between the cases analysed. The best way to achieve this without compromising the generalisability achieved by utilising and extending upon Samuel's taxonomy was to select case studies involving hacktivism being used in

aid of a particular cause. My selection of this 'binding cause' is based upon what I view as an increasingly false dichotomy within the literature on hacktivism.

2.2.3.1 A rationale for the 'binding cause' for the case studies

Jordan and Taylor (2004), in their explanation of mass action hacktivism (MAH), and digitally correct (DCH) hacktivism, categories that are subsumed into Samuels' tripartite taxonomy, argue that digitally correct hacktivists are generally more interested in the 'bandwidth rights' component of human rights than their mass action counter parts. While they are correct in identifying tension between the two groups in terms of how their actions affect the Internet architecture (a tension that is also noted by Samuel and Vegh (both 2003)), bandwidth or Internet rights, in terms of unhindered Internet access, and in terms of the struggle for control over the Internet architecture and content, are becoming increasingly inseparable from human rights as a whole. This struggle is bound up with the basic human right detailed in Article 19 of the 1948 International Declaration of Human Rights:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.
>
> ('The International Declaration of Human Rights')

The Internet is increasingly the medium through which many of us seek, receive and impart information, as well as practise our freedom of opinion and expression, not to mention conduct many more mundane aspects of daily life. Furthermore, it is through this exchange of knowledge and facilitation of activity that many other basic human rights are increasingly facilitated and upheld. As such, holding

bandwidth or Internet rights separate from other human rights is increasingly erroneous, and is only likely to become more so.

This perspective and belief is corroborated by much recent research. The Pew Internet and American Life Project has published research report after research report, all freely available on their website, confirming the increasing importance of Internet access to people's daily lives, and particularly their political lives ('Pew Internet and American Life Project'). We increasingly access news, information and other media of all kinds via the Internet (Purcell et al. 2010), from a multitude of traditional and alternative media sources. We also engage with governmental information and services online (Smith 2010), both for activities of everyday life and during election campaigns. Indeed, over half of the adult population of the Unites Sates of America went online to get involved in the political process or to get news and information about the 2008 presidential election (Smith 2009). This trend towards political engagement via the Internet is particularly strong amongst young people (Kohut 2008; Smith et al 2009), suggesting that the trend is only likely to accelerate.

There is no doubt that the selection of this cause, and the cause itself, exhibits a post-industrial bias. In a world where many have yet to achieve access to basic necessities such as adequate water, nutrition and shelter, let alone telephone connections or Internet access, focusing on struggles over unhindered Internet access, and over the governance of Internet architecture and content, may seem at best, ignorant, and at worst, arrogant. Indeed, even amongst those who do have Internet access, the demographics of political and civic involvement continue to echo offline biases towards those with higher levels of income and education – although the trend towards blogs as prominent sources of information, and political activity on social networking sites amongst younger netizens hints at possible upheavals within these participatory demographics (Smith et al. 2009). However, hacktivism is already a privileged activity – it occurs on the Internet, and is done by citizens who have Internet access in terms of both a physical connection and technological know-how and skills. As such, this thesis is already biased towards a post-industrial perspective and topic.

Furthermore, hacktivism involved in struggles over the control of the Internet tends to be aimed at securing an ideal Internet that the hacktivists see as best serving citizens, as opposed to governmental or corporate elites. As such, it is aimed at preserving, promoting and maintaining an ideal Internet not only for current, but also prospective or future 'netizens'. And there is no doubt that citizens on both sides of the digital divides (Selwyn 2004; van Dijk & Hacker 2003) recognise the importance of Internet as a communicative medium. The BBC World Service recently commissioned a survey (administered by GlobeScan) of over 27,000 adults across 26 countries, only 14,000 of whom were actually Internet users, asking them about their perceptions of the importance of the Internet to modern life ('Global Poll on Internet Access' 2010). A massive four in five adults (78%) saw access to the Internet as a fundamental human right, with 87% of the Internet users and 71% of the non-Internet users surveyed holding this opinion (ibid.: 1).

Indeed, this belief is something that has been legislatively ratified by several nations, with Finland, France and Estonia making Internet or broadband access a human right for their citizens. Internet-using respondents to the BBC survey valued the Internet most highly for sourcing information of all kinds, and for communicating and interacting with other people. 90% and 78%, respectively, felt that the Internet was a good place to learn and that it gave them greater freedom (ibid.: 4). As the BBC's Bill Thompson summarised:

> As a long-time contributor to Digital Planet, the BBC World Service programme about the impact of digital technology on people's lives, I've seen the growing awareness within the developing world that computers and connectivity matter and can be useful. It's not that computers matter more than water, food, shelter and healthcare, but that the network and PCs can be used to ensure that those other things are available.
>
> (Thompson 2010)

Further research provides more evidence of this across-the-board belief in the importance of Internet access, and particularly high-speed Internet access. The

Social Science Research Council (SSRC) recently researched the adoption of broadband in low-income American communities (including homeless citizens and those relying on governmental welfare for survival). While previous research (mostly quantitative and survey based) done by the Pew Internet and American Life project has identified various proportions of non-Internet users who do not use the Internet because they see it as 'not relevant' to their daily lives, the SSRC research, which had a smaller sample size but engaged research subjects much more deeply, using a combination of qualitative and quantitative methods, found a different reality:

> …we found no such group, even among respondents with profound histories of marginalization—the homeless, people with long-term disabilities, people recently released from lengthy prison sentences, non-English speakers from new immigrant communities, and residents of a rural community without electricity or running water. No one needed to be convinced of the importance of Internet use or of the value of broadband adoption in the home.
>
> Indeed, most respondents viewed broadband connectivity to be of paramount importance. Over 90% of our non-adopter respondents reported personally using the Internet. Taking into account proxy use via family members and friends, the number approaches 100%. Even respondents with the highest barriers to use, such as those with very limited literacy in any language, reported making efforts to use the Internet. Social networking, games, and media sites—especially YouTube – seem to be common gateways for these low-skill users. But the strongest drivers by far among our respondents are access to employment, education, and government services.
>
> (Dailey et al. 2010: 15)

Clearly, those on both sides of the digital divides share a belief in the importance of Internet access, and particularly high-speed Internet access. Those who do not have Internet access know they are missing out, and their numbers are decreasing constantly (and will hopefully continue to do so apace). We still have a long way to go before we can claim global connectedness, but there is a strong sense that this is a goal of fundamental importance. While hacktivism in the name of debating

control over the Internet's architecture and content is not directly involved in securing broader Internet access, it is engaging with rights that should not be set aside from other 'offline' rights. The Internet is part of and generated by a significant proportion of modern humanity, and deserves to be recognised in terms of general human rights, rather than set aside as something important only to the privileged, particularly as access continues to grow. We would do well to remember that:

> [t]he Internet is only that wire that delivers freedom of speech, freedom of assembly, and freedom of the press in a single connection. It's only vital to the livelihood, social lives, health, civic engagement, education and leisure of hundreds of millions of people (and growing every day).
>
> (Doctorow 2008)

As such, I believe that the selection of this particular 'binding cause', while certainly following the post-industrial bias of this thesis in general, is not as elitist as it may initially appear. Certainly, hacktivism is a form of protest used by and differentially available to a technological and socio-economic elite, and on what is still a (globally) technologically and socio-economically elite medium. But as access to the Internet is ever-increasingly accepted as a fundamental human right (even if, like many other rights, it is not globally upheld in actuality), hacktivism engaging with this cause is arguably little more elitist than that engaging with many other causes. Furthermore, given that this cause is inherently associated with the very platform upon which hacktivism occurs, and that the increasing 'mainstreaming' of unhindered Internet access as a fundamental human right goes some way towards bridging the schism between the trends of mass action and digitally correct hacktivism identified by Jordan and Taylor (2004), it is hoped that it is seen as a considered and logical choice for providing cohesion between the following case studies.

As such, the three cases (as depicted in Tables 2 to 4) were theoretically sampled using Samuel's typology, and the 'binding cause' of the struggle for control over

the current state and evolutionary future of the Internet. No further detail on each case will be provided at this stage, as the analysis of each will necessarily provide a detailed description of them. For now, it is sufficient to see that each case deals primarily with a single category within Samuel's hacktivist taxonomy, and that in combination, the three cases cover the vast majority of the variations within Samuel's typology of hacktivism (2004a). Bold entries indicate specificities within cells with multiple variations, and unknown variations are indicated with italics. The tables representing each case are placed so as to avoid breaking across pages.

2.2.3.2 Case One: Hacktivismo

VARIATIONS / TYPE OF HACKTIVISM	POLITICAL CRACKING	PERFORMATIVE HACKTIVISM	POLITICAL CODING
(1) ORIGIN	Hacker-programmer	Artist-activist	**Hacker-programmer**
(2) ORIENTATION	Outlaw	**Transgressive**	
(3) NYMITY PRACTICES	Robust pseudonymity	Use real names	**Weak pseudonymity**
(4) GROUP SIZE	Solo or small	**Medium**	
(5) COLLABORATIVE SCOPE	National, multinational or international	**Multinational**	
FORMS	Defacements Redirects Automated DDoS attacks Sabotage Information theft	Parodies Sit-Ins	**Software development**

Table 2: Hacktivist variations within the case of Hacktivismo

2.2.3.3 Case Two: The Creative Freedom Foundation and the New Zealand Internet blackout

VARIATIONS / TYPE OF HACKTIVISM	POLITICAL CRACKING	PERFORMATIVE HACKTIVISM	POLITICAL CODING
(1) ORIGIN	Hacker-programmer	**Artist-activist**	Hacker-programmer
(2) ORIENTATION	Outlaw	**Transgressive**	
(3) NYMITY PRACTICES	Robust pseudonymity	**Use real names**	Weak pseudonymity
(4) GROUP SIZE	Solo or small	**Medium (to large)**	
(5) COLLABORATIVE SCOPE	**National**, **multinational** or international	**Multinational**	
FORMS	**Defacements** **Redirects** Automated DDoS attacks Sabotage Information theft	**Parodies** **Sit-Ins**	Software development

Table 3: Hacktivist variations within the case of the Creative Freedom Foundation and the New Zealand Internet blackout

2.2.3.4 Case Three: Anonymous and Australian Internet censorship

VARIATIONS / TYPE OF HACKTIVISM	POLITICAL CRACKING	PERFORMATIVE HACKTIVISM	POLITICAL CODING
(1) ORIGIN	**Hacker-programmer**	Artist-activist	Hacker-programmer
(2) ORIENTATION	**Outlaw**	Transgressive	
(3) NYMITY PRACTICES	**Robust pseudonymity**	Use real names	Weak pseudonymity
(4) GROUP SIZE	Solo or small	**Medium (to large)**	
(5) COLLABORATIVE SCOPE	*National,* ***multinational*** *or international*	**Multinational**	
FORMS	**Defacements** Redirects **Automated DDoS attacks** Sabotage Information theft	Parodies **Sit-Ins**	Software development

Table 4: Hacktivist variations within the case of Anonymous and Australian Internet censorship

2.2.3.5 The overall representativeness of the case studies

VARIATIONS / TYPE OF HACKTIVISM	POLITICAL CRACKING	PERFORMATIVE HACKTIVISM	POLITICAL CODING
(1) ORIGIN	**Hacker-programmer**	**Artist-activist**	**Hacker-programmer**
(2) ORIENTATION	**Outlaw**	**Transgressive**	
(3) NYMITY PRACTICES	**Robust pseudonymity**	**Use real names**	**Weak pseudonymity**
(4) GROUP SIZE	Solo or small	**Medium**	
(5) COLLABORATIVE SCOPE	**National, multinational** or international	**Multinational**	
FORMS	**Defacements** **Redirects** **Automated DDoS attacks** Sabotage Information theft	**Parodies** **Sit-Ins**	**Software development**

Table 5: The overall representativeness of the three case studies

All bar one cell or defined variation within hacktivism is shaded if the three case studies are taken as a whole; hence, they work in combination to provide a representative sample of hacktivism, as is represented by Figure 5. The omission of a case of hacktivism carried out by a small group or lone individual is regrettable, but given the difficulty of actually ascertaining how many hacktivists are involved with or behind certain actions, particularly in cases of political cracking (carried out by individuals using robust pseudonymity), is not seen as overly problematic. The lack of coverage of a case of international engagement is also compensated for by the fact that two out of three of the possible variations within collaborative scope are represented, and especially given that these variations are much more inconsistent than the main taxonomic variations of hacktivist origin and orientation.

In line with this variability and lack of fixedness within types, each case study is predominantly aligned with a single category within Samuel's hacktivist typology, but there are some areas of category permeation, thus the cases provide evidence of the taxonomic fluidity possible within hacktivism. Not all forms of hacktivism are represented or discussed – within the category of political cracking, sabotage and data theft are not addressed – but given the diversity of hacktivism, this is hardly surprising. The broader structural and taxonomic variations are accounted for, and furthermore, covering each and every form of hacktivism through critical discourse analysis would be too large a project. As such, these three case studies aggregate into a theoretically selected and sufficiently representative sample of hacktivism as whole.

2.2.3.6 The selection and collection of a data corpus for each case study and critical discourse analysis

As previously outlined, the three cases are analysed using a critical discourse analytic methodology. As such, a corpus of data on each case was necessary to provide both contextual information and a text or texts for close analysis. The selection and collection of this corpus used a necessarily flexible technique – each case study had different documents associated with it, so there could be only a flexibly defined central method of collecting data or texts for each.

Hacktivism is not something that is always represented by discrete texts – it is something that is re-presented or recounted through secondary accounts and archived traces of the hacktivism. As such, the data for this aspect of the research question was generated using whatever useful and reliable material could be found – screenshots of defaced pages; mainstream and alternative media accounts; statements from targets; software; information disseminated by hacktivist groups or individuals by way of websites, forums or other texts – essentially, any textual or visual artefact that contributed to a better understanding of the hacktivism. As

many artefacts as possible were used to build an understanding of the form of the hacktivism that took place, in order to overcome any possible omissions or inaccuracies present in any one artefact. In the case of the Creative Freedom Foundation, I also interviewed one of the founders of the group (Bronwyn Holloway-Smith) to gain background information unavailable elsewhere. This was made possible both by her geographical accessibility (being based in New Zealand) and willingness to discuss their (definitively legal) hacktivist campaign.

The selection of texts for close analysis used similar methods, but was limited to records of textual or visual statements produced by the hacktivists pertinent to each case. These include screenshots of defaced pages; mainstream or alternative media reproductions of email statements issued, or other hacktivist-produced textual messages otherwise archived; software; and information disseminated by hacktivist groups or individuals by way of their websites, forums or other texts. Due to this necessarily eclectic method and variance between cases, the specific text or texts selected for close analysis in each case is further clarified and specified within the critical discourse analysis itself.

2.2.4 Research questions

2.2.4.1 A 'theoretical turn': Research question 1

As previously outlined, I initially intended to apply Habermas's criteria of communicative rationality to hacktivism to ascertain whether or not it fulfilled the criteria for inclusion into the Habermasian public sphere. However, the more I researched the theory of the public sphere, the more it became apparent to me that there were grave issues with the Habermasian ideal. Although some of the literature stemming from the Habermasian public sphere involved applying the rational-critical procedural criteria to different situations, such as online forums, and

assessing their degree of democratic communicative legitimacy, the vast majority of it was more concerned with critiquing the public sphere in both its pre- and post-linguistic turn iterations. I became increasingly uncomfortable with the thought of uncritically accepting the Habermasian ideal as an appropriate yardstick by which to measure legitimate public sphere activity. At the same time, I began to identify repetitive themes within the critiques I was reading, and in related deliberative democratic literature, in terms of both their deconstructive and reconstructive intent.

This resulted in a 'theoretical turn' within my research, as the sheer mass of criticism aimed at the Habermasian ideal, combined with the lack of any 'joining of the dots' between the literature in the 'post-modern', 'radical', or 'agonistic' public theoretical tradition led me down the route of a theoretical synthesis project. Rather than simply accepting and operationalising the Habermasian ideal, in the form of the rational-critical procedural criteria, I began to work on synthesising the aforementioned theoretical tradition, with the intent of constructing a holistic and concisely definable 'new' public sphere model. As such, the first research question posed and answered by this thesis is:

> *R1: How can the critical democratic intent behind the Habermasian ideal of the public sphere be reconciled with both:*
>
> *a) the practical and theoretical criticism levelled at it, and*
>
> *b) the diverse reconstructive projects undertaken within the 'post-modern' 'radical' or 'agonistic' public sphere and deliberative democratic theoretical traditions, which attempt to remain sensitive to issues of difference and power;*
>
> *in a manner that generates a concise, holistic and operationalisable definition of the public sphere, that accounts and is appropriate for the modern mediated communicative environment?*

The theoretical framework constructed in Chapter 6 provides the answer to this question, and also establishes that hacktivism, be definition, fulfils the criteria for

being a legitimate form of participation within the global network of neo-Habermasian public and counterpublic spheres.

This framework also made it clear that there were two 'public sphere orientation' based perspectives I could take on hacktivism. Neo-Habermasian public sphere theory envisages neo-Habermasian publics and counterpublics as being public in that they have an outwards orientation – they aim to engage with other public spheres – as well as having an inwards, group-solidarity-based orientation. As such, I needed to decide which orientation I was most interested in investigating. The latter orientation would be aimed at uncovering the internal solidarity mechanisms of hacktivist groups and associations. However, there were two problems with this option. Firstly, Samuel (2004a) had already done an extensive and admirable investigation into the identity and group-solidarity based aspects of hacktivism. Secondly, I was not particularly interested in an explicit exploration of this aspect of publics, hacktivist or otherwise. I was and continue to be more interested in how they present themselves to their targets and audiences – how they construct the external manifestations of their counterpublicity, and to what end.

2.2.4.2 Hacktivism as counterpublic spheres: Research question 2

As such, the second research question this thesis explores is:

> *R2: How does hacktivism, through discursively constructed and externally oriented publicity, function as a counterpublic sphere or counterhegemonic project oriented towards the provocation of political preference reflection and the destabilisation of a given dominant or hegemonic public?*

Neo-Habermasian public sphere theory (and indeed, any conception of the public sphere) sees publics and counterpublics as discursively constructed. Political conflicts, and thus interactions between counterpublics, are foremost discursive struggles, with discourses generally understood as "shared set[s] of concepts, categories, and ideas that provide [their] adherents with a framework for making sense of situations, embodying judgments, assumptions, capabilities, dispositions, and intentions" (Dryzek 2006: 1). However, hacktivism clearly effects the discursive construction of counterpublics in inventive and creative ways. As such, this second research question can be further segregated into two parts, which will both be explored using the previously outlined critical discourse analytic methodology:

> *R2.1: How does the discursive **form** of hacktivism, as a counterpublic sphere or counterhegemonic discursive project, contribute to the provocation of political preference reflection and the destabilisation of a given dominant or hegemonic public?*
>
> *R2.2 How does the discursive **content** of hacktivism, as a counterpublic sphere or counterhegemonic discursive project, contribute to the provocation of political preference reflection and the destabilisation of a given dominant or hegemonic public?*

Having defined the methodology and the research questions, we will now proceed to a review of the literature on hacking and hacktivism, thus establishing that an investigation of hacktivism through a public sphere theoretical lens is a valid and compelling research direction.

Chapter 3

The evolution and current form of hacking: An investigation of existing knowledge

Fundamentally, hacktivism can be defined as the following:

hacktivism = Internet (hacking + activism)

That is, it is the melding of various combinations of the techniques and ideologies of traditional social activism with various combinations of the techniques and ideologies of hacking, as practised in the context of the Internet.

However, the reality is, inevitably, much less simple. For instance, it should be immediately noticeable that, in contrast to the usual mediated representation of hacking, the activity is not necessarily set within the context of the Internet. As such, an in-depth investigation into the history of and literature on hacking is necessary to obtain a firmer grasp of what this dynamically evolving and variously perceived practice and its associated terminology actually constitute. As will be shown, this is no easy task - the origin of the term and the identity it refers to are both obscure, as it has been and is used in a variety of contexts and connotations.

This literature review, which is embellished with excerpts from interviews and personal communication[1] with organisers and attendees of the first New Zealand hackers conference, Kiwicon, in November 2007 ('Kiwicon'), does not aim to achieve a simultaneously detailed and concise definition of either the hacker or hacking – that is an impossible task. Instead, the floating polysemy of the term will be fully explored, generating a multi-layered and dynamic theoretical concept that illustrates the praxis and identity of hacking more accurately than any brief

[1] All communications are [*sic*] – i.e. any errors in quotes from Kiwicon attendees have been reproduced verbatim from the original communication, and are not transcription errors. Furthermore, the hackers spoken to were given a choice of identifying themselves by their real

definition. This exploration will provide the context for the ensuing review of hacktivism.

3.1 The emergence and evolution of hacking: Motivations and perceptions

Since its emergence into popular consciousness, computer hacking is a concept and activity that has captured the attention of both academia and the public imagination, as well as having obvious significance to those who practise it (and are exposed to it). Indeed, "[h]acking is undoubtedly one of the buzzwords of the computer age" (Vegh 2003: 151). However, "[t]he origin of the word is obscure, and the term has been used to mean rather different things" (Cornwall 1987: 18), and as such, the definitions of the action and its actor, the hacker, remain mercurial.

Even hackers, when asked to define the activity, have extremely varied responses, as is shown by the statements of the New Zealand hackers spoken to. One describes hacking in such a way that it was clear he sees it as involving gaining access to some system (presumably a computing system) that you are not supposed to have access to – the access is gained through:

> [t]he use of security exploits, holes and ignorance. It can also be used to describe quick fix solutions for software (getting rarer now though).
>
> (Parsons 2007)

The second part of his statement refers to a more archaic or specialised usage – one that is not generally recognised by the media, as we shall see - and one that he feels is falling from fashion. There is a clear self-awareness as to the floating polysemy of the term – the term 'hacking' can be used to describe more than one activity, and

its meaning has changed (and is still changing) over time. Another hacker, one of the organisers of the conference, described hacking in purposefully vague terms, as:

> …gaining control of the target.
>
> (Bogan 2007)

There is no presupposition of either target or intent – diverse targets can be hacked using diverse means and for diverse ends, but these means and ends always presuppose an achievement of control or mastery. This open-endedness was more fully elucidated by one of his fellow organisers, who further differentiates the action of hacking from the various human qualities driving it:

> Hacking in the strict computer sense I see as a manipulation of the technology to perform some action that was unintended by the designers/operators.
>
> In a larger sense, I see hacking as an expression of curiosity and a desire to understand the operation of complex systems, in the same category as other enthusiasts.
>
> In neither case do I include motivation or ethics as part of the definition – these are qualities of people, not hacking.
>
> (Metlstorm 2007a)

In line with this, the answer to the double-question "What is a hacker? Aren't hackers bad?' provided in the Kiwicon FAQ reveals a wider group corroboration of the polysemy of the hacker identity and associated activity. It also recognises the very specific and therefore limited media portrayal of hackers, a phenomenon much discussed within the following literature review:

> Hackers are compulsive destroyers of "Warranty Void if Broken" stickers. They are people who enjoy exploring, understanding, and using technology creatively. Many hackers are interested in the security of computer systems, but as technology develops, hackers of different kinds are pushing the limits of cars, gadgets, and various media.
>
> However, the general perception of a 'hacker' is synonymous with 'computer criminal', and indeed some computer criminals are hackers. However, the prevention of electronic crimes and the defenses of modern networked systems are ensured by computer security professionals; the best of whom will often self-identify as hackers!
>
> Hackers value elegant, creative and often playful solutions to technical challenges; combining the role of inventor and artist in an industry that many laypeople would consider staid. In a world where society's technological dependence is as obvious as the technology itself is opaque, hackers provide the tools and language for social conscience, balance and freedom.
>
> ('Kiwicon FAQ')

This polysemy, and tendency towards abstract as opposed to concrete forms of definition are in evidence throughout the academic literature on hacking. Both the origin of the terms 'hacking' and 'hacker' and the identity they refer to is obscure, and they have been and are used in a variety of contexts and connotations. Indeed, the concept of meaning 'all things to all men' could scarcely be more applicable. As such, a comprehensive examination of the central literature pertaining to the subject is prerequisite to a holistic and multi-dimensional appreciation of its core theories, practices and debates.

Literature on hacking began to emerge in the mid Eighties, as the computer and the idea and growing reality of personal computing began to insert itself more firmly into public discourse. While computers had been in existence for some time in one form or another, it was only during the Seventies and Eighties that they began their transition from exclusively institutional and often massive mainframe equipment into the more compact and multi-functional personal computers familiar to us today. As computers became more widely accessible and penetrable to individuals other than those holding engineering degrees and associated with institutional computer-owners – a paradigm shift in part effected by hacking itself – their role and

prevalence in daily life became ever more pronounced. This generated more hackers, as well as a public more likely to find discourse on the practice interesting and relevant.

Accordingly, a number of texts, ranging in tone from pseudo-academic to definitively populist, emerged throughout the Eighties and early Nineties examining the 'hacker phenomenon'. Some notable examples are Levy (1984), *Hackers: Heroes of the Computer Revolution*; Hafner & Markoff (1991), *Cyberpunk: Outlaws and Hackers on the Computer Frontiers* (written by a pair of American journalists); Mungo & Clough (1992), *Approaching Zero: The Extraordinary Underworld of Hackers, Phreakers Virus Writers and Keyboard Criminals* (written by a pair of British journalists); Sterling (1992), *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*; and Slatella & Quittner (1995), *Masters of Deception: The Gang that Ruled Cyberspace*.

These texts make for interesting and entertaining reading, and offer some valuable insights into early hackers and hacking practices, often from a personally familiar viewpoint. However, as might therefore be expected, none of these are exactly objective examinations of the practice. They tend to take a distinctly idealistic and even affectionate perspective, presenting hackers as likeable figures despite their sometimes-criminal activities – the Robin Hoods of the computer world. This mythologising tendency is apparent throughout the literature on hackers, though the more academic and therefore more valuable texts attempt to deconstruct the myth to get at the realities behind it, as well as examining the process of its construction.

Nevertheless, some of these texts will be referred to in passing to take advantage of various discrete insights, and one in particular is worthy of more thorough review. This is Stephen Levy's (1984) *Hackers: Heroes of the Computer Revolution*. It is notable in that a significant proportion of the academic literature on hackers refers back to general categorisations and summations made by Levy. *Hackers* is essentially a historical account of the early years of hacking throughout the Fifties, Sixties and Seventies. It constitutes an examination of what has retrospectively been referred to as the first three generations of hackers, or 'First Wave' (Chandler (1996), Jordan (2001, 2004), Jordan & Taylor (1998, 2004), Taylor (1998, 1999, 2000).

3.1.1 Generation one: The true or original hackers

These were "the pioneering computer aficionados who emerged in the earliest days of computing" (Jordan & Taylor 2004: 10), and experimented with mainframe computer capabilities during the Fifties and Sixties at such academic institutions as MIT, UC Berkeley, Carnegie-Mellon, Cambridge, and Stanford. Many of these individuals were not allocated or did not require significant computer access as part of their study; rather, they had to inveigle access to the mainframe equipment of the time, such as the TX-0, PDP-1 or the PDP-6. Their applications of their allotted time were various, an example being the Model Tech Railroad Club who saw computing as a way to enhance the functions of their beloved trains, but their usage became increasingly focused on expanding and enhancing the capabilities of the computing equipment they had access to. "To the hackers, the system was an end in itself" (Levy 1984: 117). These individuals, painted as obsessive yet lovable misfits by Levy, were responsible for the evolution of the earliest programming techniques. They were "tolerated with grudging admiration" (Nissenbaum 2004: 198) and respect by the other students and staff, many of whom had superior access to the equipment, but were routinely outstripped in skill and achievement by the 'hackers'. The significance of their occasionally semi-illicit access to and usage of this institutional equipment was even wryly acknowledged by Defensive Advanced Research Projects Agency (DARPA), who provided funding intended for 'legitimate' study at MIT (Levy 1984: 122).

3.1.1.1 The contested nature of 'the hack'

Levy also introduces the contested nature of the hacking terminology, another concept that is recurrent throughout the literature. He acknowledges that its true origin is obscure, but identifies the term 'hack' as 'ancient' MIT lingo for an elaborate practical joke, such as covering the campus dome with tin foil. Thus, a

hack designated a project with no real constructive goal, just a "wild pleasure taken in mere involvement" and "imbued with innovation, style and technical virtuosity" (1984: 9-10). This tradition continues today, and is chronicled on the MIT *Interesting Hacks to Fascinate People Gallery* website ('IHTFP Hack Gallery'). The site FAQ specifically contests the common understanding of hackers as "people that break into computer networks", asserting that a hacker is rather "someone who does some sort of interesting and creative work at a high intensity level. This applies to anything from writing computer programs to pulling a clever prank that amuses and delights everyone on campus" (ibid.)

Notably, this original connotation does not necessarily have anything to do with computers – the object or subject of the hack is undefined. Although current understandings of the term tend to lock in an association with computing of some kind, this initial non-specificity persists in many ways, contributing to the mercurial terminological status of the activity. Much hacking involves some element of 'wetware' hacking or social engineering, thus maintaining a link to both the ephemerality and prank-relatedness of the original term. It is also not uncommon within certain circles (generally those with some connection to computing technology) to refer to any kind of playful, creative, ingenious interaction, modification or manipulation of an object or subject as hacking. The popular website *Lifehacker* is a well-known example ('Lifehacker'). It dispenses advice on how to hack various elements of ones' life – computers, certainly, but also food, clothes, homeware, even oneself - in the interests of greater productivity. This trend towards productivity or purposiveness, although not originally a factor, has intensified with the chronological evolution of the hack, and was apparent in even the first generation or original hackers. However, the other characteristics of pleasure, style, innovation and virtuosity also remain integral.

3.1.2 Generation two: The hardware hackers

Levy's second generation are "the computer innovators who, beginning in the 1970's, played a key role in the personal computing revolution which served to widely disseminate and dramatically decentralise computing hardware" (Jordan & Taylor 2004: 10). This generation was odd in that it was both countercultural and commercial – helping to bring computing power to the people, but also managing to generate some significant profits. Groups such as the Homebrew Computer Club developed the first kitset or fully assembled personal computers, and began selling to the public. It must be acknowledged that this 'public' was still largely comprised of professional or amateur electronics enthusiasts, but the ideological impetus and technical development was towards equipment that would allow 'Joe (or Jane[2]) Public' to take part in the 'computer revolution'.

Some enterprises were spectacular examples of mismanagement and failed, but others succeeded equally as spectacularly. Perhaps the most widely cited example of this was Apple Computers, headed by the young Steven "Woz" Wozniak and Steven Jobs, a "[v]isionary, bearded, non-hacking youngster who took Wozniak's Apple II, made lots of deals and formed a company that would make a billion dollars" (Levy 1984: xiii). Many of the millions of Apple fans clutching their iPads™ and iPhones™ today are doubtless unaware that their gurus' business began by selling 'little blue boxes' that allowed the user to hack into the phone system using specific tonal frequencies and thus place free phone calls. This practice, commonly referred to as 'phreaking', is a good example of extra-computer hacking, with the infamous John Draper (a.k.a. 'Cap'n Crunch'[3]) its most well known proponent.

---

[2] Although it is worth noting that Levy's book paints an almost exclusively masculine profile of hackers. This is no oversight or prejudice on his behalf, simply a reflection that the community was and indeed, is, largely male.

[3] Draper was known by this moniker due to his having found that if he held his finger partially over the end of a toy whistle found in a carton of 'Cap'n Crunch' breakfast cereal, he could generate a tone of the exact frequency needed (2,600 hertz) to trick the phone system, which worked via tonal recognition, into effectively thinking that a toll call had been terminated and thus returning to operator mode, whereupon Draper could 'phreak' his way through the phone system at no cost. He was eventually charged with telecommunication fraud.

Levy depicts these hardware hackers as almost single-handedly bringing 'computing power to the people', and indeed, statements made by the heads of various computing firms at the time indicate their lack of vision (in Himanen 2001: 187):

> I think there is a world market for maybe 5 computers.
>
> (Thomas Watson, president of IBM, 1943)

> There is no reason anyone would want a computer in their home.
>
> (Ken Olsen, chairman of Digital Equipment Corporation, 1977)

However, the maximal credit Levy attributes to hackers in the process of disproving this perspective is disputable. Pre-existing large corporations did have a large role to play in the distribution of computing. Nonetheless, it may be fairly argued that the 'hardware hackers' did provide a significant driving force as well.

3.1.3 Generation three: The software or game hackers

This third generation were "innovators who focused more and more on elegant means of changing or creating programs to run on the hardware being hacked up, often by their friends or colleagues, the hardware hackers" (Jordan & Taylor 2004: 10). They were responsible for leading the evolution of computer game architecture, sometimes pirating copies of existing game software in order to 'hack it up' into a more advanced version. Unlike the previous generations, their motivations were not entirely altruistic; while some of the hardware hackers did make massive profits, they were largely unforeseen by-products of their desire to diffuse computing throughout society. For many game or software hackers, "[t]heir

motivation was a fast buck, and their instincts were often entirely commercial" (Mungo & Clough 1992: 74). Here we can begin to see a subtle shift in the definition of 'hacker', with notes of personal gain and the further suggestion of illicit activity creeping in. This shift in ethics, both perceived and actual is significant, as we shall see.

3.1.3.1 The hacker ethic

In addition to delineating these first three generations, Levy also introduced the idea of the hacker ethic, and provided an elucidation of its core tenets. This categorisation has been frequently cited throughout the subsequent literature on hacking, and is worth reproducing in full:

> 1) Access to computers – and anything which might teach you something about the way the world works – should be unlimited and total. Always yield to the hands-on imperative!
>
> 2) All information should be free.
>
> 3) Mistrust authority – promote decentralisation.
>
> 4) Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
>
> 5) You can create art and beauty on a computer.
>
> 6) Computers can change your life for the better.
>
> (Levy 1984: 27-33)

Tenets two and three bear further comment. The idea that all information should be free was grounded in the fact that computers need an unhindered internal flow of information if they are to work optimally, but has come to signify much more. It is

now widely understood as standing in opposition to the increasingly corporate-friendly regulation of intellectual property, and as advocating the free flow of information generally, usually in the context of the Internet. As such, this challenging ethic will crop up in further literature under review. The third tenet is related in its critique of bureaucracy and corporate hierarchy, with IBM - "The Enemy" – and its hated "batch-processed and intolerable" IBM 700, the epitome of corporate dominance and bureaucratic inefficiency and inelegance (Levy 1984: xiii). Furthermore, the advocacy of decentralisation has become of utmost relevance in the context of the Internet, and provides further conflict concerning intellectual property and other corporate agendas. Despite Levy's informal style and non-academic approach, the discussed concepts and categories provide an invaluable starting point for the ensuing academic literature under review, and Levy's work has been given prominence and relied upon by most academics since. As such, his work and concepts are more than worthy of inclusion.

3.1.4 Generation four: The hacker as criminal (a.k.a. the cracker)

The next notable subtopic within the literature and generation within hacking's evolution is dealt with in Hollinger & Lanza-Kaduce's (1988) 'The Process of Criminalisation – The Case of Computer Crime Laws', in which they dichotomise Levy's hacker ethics and newly developed cybercrime legislation. The ongoing criminalisation and pathologisation of hacking (both legal and reputational) is linked in with a fourth generation of hacker, both actual and imagined – the hacker/cracker. This generation, and the generations five through seven to follow, are typological extensions to Levy's (1984) first three generations, and are outlined later in Jordan and Taylor (2004). These extensions, despite having a temporal or chronological dimension, are not seen as mutually exclusive – rather, they identify different ideological subgroups within hacking, and are immensely useful in terms of grasping the diversity and evolution of the practice.

This fourth generation embodies the illicit nature of the hack, and its members are largely defined by their intent to achieve unauthorised access to computers and networks. This unauthorised access can be in pursuit of personal gain or out of sheer destructive malignancy, but can also be driven by more benign motivations, such as curiosity, challenge, or a desire to reveal (and thus prompt the patching of) weaknesses in computing systems. This generation and the issues it generated will be discussed in more detail, but suffice to say, hacking was and continues to be of increasing concern to both the public, and governmental and corporate institutions. Hollinger and Lanza-Kaduce's text surveys the new legislature and regulations being installed in an attempt to define and control the legal limits of the new computer environment, and the resulting effective criminalisation of hacking involving unauthorised computer entry (regardless of motive). Beyond this basic lack of consideration for intent, these laws were often incompletely thought out and ineffective for a number of reasons, a tendency elaborated upon in ensuing literature on the subject.

Further literature addresses hacking from this criminological/legal perspective, such as Johnson's (1994) *Crime, Abuse and Hacker Ethics* and Loper's (2001) thesis, *The Criminology of Computer Hackers*, with the disjunction between hacker ethics and legislation often central to the discussion. These texts are part of a larger subset of literature found within computer industry, business and military publications, which tends to disregard any discussion of motive, and often considers hacking as criminal by default. Some notable examples are: Adams (1996); Evers (1996); Furnell (1999); Hancock (1998); Neighly (2000); Onstad & Rose (1996); Richardson (1997) and Weisenburger (2001). This literature is of limited usefulness here, as it involves little discussion of the hackers or hacking themselves, and focuses rather exclusively on potential preventative and protective measures to be taken against them and their actions.

3.1.4.1 The media and the beginning of the myth of the 'electronic bogeyman'

Hollinger & Lanza-Kaduce (1988) are also important in that they note the importance of the news media in the criminalisation process - specifically, the way in which their sensationalistic coverage of hacking fuels public concern and has often prompted new legislation and amendments to pre-existing legislature. This 'electronic bogeyman' (Smith 2001: 66)[4] phenomenon is of central importance throughout the literature to be discussed; hence, this early recognition of the trend is notable. It had been acknowledged in some of the earlier populist texts, such as Hafner & Markoff (1991), but this was arguably the first academic identification of the phenomenon and is therefore significant, despite its lack of empirical evidence.

Amanda Chandler's (1996) essay, 'The Changing Definition and Image of Hackers in Popular Discourse' continues in this theme, discussing the mass-mediated images of hackers in the U.S.A. and Britain. Chandler acknowledges the contested definitional nature of the hack, and drawing on Levy's (1984) first three generations and the work of Hafner & Markoff (1991) and Clough & Mungo (1992), explicitly recognises the fourth generation, who "appropriated the word 'hacker' and with help from the press, used it to define themselves as password pirates and electronic burglars. With that, the public perceptions of hackers changed. Hackers were no longer seen as explorers, but as malicious intruders" (Hafner & Markoff 1991: 11). The emergence of computer viruses and worms and their usage by hackers in the Eighties had further entrenched this actual and perceptual paradigm shift. Chandler identifies five categories of image as prevalent in the mass-mediated representation

[4] "[E]lectronic bogeyman: a hacker, instrument of a hacker, or anonymous source portrayed in the mainstream media as a menace to society." (ibid.. in main text) Smith's text is a chapter entitled 'Upon Hearing of the Electronic Bogeyman', in *You Are Being Lied To: The Disinformation Guide to Media Distortion, Historical Whitewashes and Cultural Myths* (2001). It is a biting criticism of the perceived idiocy of the mass media and governmental and military officials with regards to hacking, citing numerous examples of endless recycling of incorrect information, including several April Fool's day hoaxes that ended up in military reports. While amusing reading, it is more an opinion piece than an academic text, and as such, will not be reviewed further.

of hackers; 'Cowboys and the Electronic Frontier', 'Intellectual Joyriders', 'Hackers/Murderers', 'Mad Hackers, and 'Spies'.

Concerning the images of hackers as cowboys on the electronic frontier, Chandler cites a number of news media sources and the Electronic Frontier Foundation ('EFF') as representative of a wider impression of hackers as heroic, mythical individuals exploring the uncharted geography of cyberspace. Their adherence to an individual code of conduct and disregard for or circumvention of computer crime legislation is also identified as parallel to the frontier ethos of the Western United States compared to the Eastern States during the 'winning of the West'. Chandler rationally posits that this image is one "for which the Americans have a sneaky admiration" (1996: 236), as is evidenced by its prevalence in American advertising and marketing.

Hackers are also linked to the 'folk devil' of the joyrider – "youngsters in stolen high-performance cars" (ibid.: 237). This association is based upon a similarity with the tendency for hackers to be young males, and to the antisocial, potentially dangerous, yet exciting nature of the practice. These connections with antisocialism and menace are extended upon by the murderous images of hackers, constructed by the news media's tendency to focus on their potential to cause fatalities – the "standard nightmare scenario" (Sterling 1993: 40) - and films such as *Die Hard 2: Die Harder* and *War Games*, in which hackers knowingly or unknowingly interfere with air traffic and nuclear weapons systems. This trend continues today, with *Die Hard 4.0: Live Free or Die Hard* revisiting the theme, and the evil robots known as 'Decepticons' in *Transformers* and *Transformers 2: Revenge of the Fallen* engaging in malicious hacking activity, not to mention the almost weekly news articles warning of impending doom via cyberwar. The pathological nature of hacking terminology (e.g. viruses, worms) also continues to embellish these images of lethality.

'Mad Hacker' images construct hackers as individuals beset by a pathological addiction or compulsion; so obsessed with computers that they are unable to take care of themselves, shy away from social interactions, and have trouble differentiating reality and fiction. Allusions to sexual voyeurism and masturbation embroider the impression of psychological instability, as do those to inhumanity.

Despite *Computer Dependency*, the 1989 study by Shotton, finding that only a very small number of computer users were dependant and that this was not necessarily a bad thing for either them or civil society, this image set was widespread, with Charlesworth's (1993) 'Addiction and Hacking' providing a unconvincing legal perspective on the concept. Indeed, it continues to have significance in the modern discourse on hacking, as part of a wider and growing concern over 'Internet addiction' that pathologises the Internet in general, as well as hacking specifically. Chandler's (1996) last image group of hackers as spies also resonates with the discourse on cyberespionage and cyberterrorism evident today (which will be further discussed shortly).

Overall, Chandler found the images to be uniformly negative in nature, although those presented in the U.S.A. were found to be slightly less negative overall, due to the tempering effect of the American-friendly cowboy and frontier images. There is no doubt that the negative representational trend identified by Chandler was and continues to be an actuality, and her selection of qualitative evidence is varied and compelling.

The same year also saw the publication of Duff & Gardiner's (1996) article, 'Computer Crime in the Global Village: Strategies for Control and Regulation - In Defense of the Hacker'. Noteworthy for their simultaneously 'pro-hacking' yet legal viewpoint, they make a legal assessment of hacking that recognises the importance of motive in the criminalisation process. They differentiate between the "clever/curious" and the "malicious/devious" (1996: 218), and acknowledge that the legal response in Britain and the U.S.A. had not yet made this distinction, nor had British or American state legislature distinguished between entry to a computer system and actual damage done. They also acknowledge the change in meaning of 'hacker', and the media's role in this process: "Hacking has become a term loved by the media who have both mythologised and demonized the hacker" (ibid.: 215), and the link with the increasing control of public space and privatization of knowledge. Their rebuttal of the arguments for criminalisation hinges upon the notions of deterrence and retribution. They address the problematic issues of detection and enforcement, and the fact that this combination of unlikely punishment and elevation of mystique may actually promote further hacking. The actual moral

status of the practice is also seen as far from clear, as 'curious' hacking may actually further security measures through the identification of system flaws, and posit that the data owner should be responsible for ensuring that system security is at least adequate.

Theirs is, indeed, a refreshing change from the usual legal perspective, and they raise some valid points, but their text suffers from a sometimes uncomfortably self-conscious use of 'cyberjargon', and one gets the sense that they themselves are less than immune to the glow of hacker mythology. As Vegh neatly summarises, "their essay is rather a journey of two law school professors into the digital underground, given their superficial understanding of hackers and cyberpunks… and their falling into the same trap of sensationalizing what they otherwise rightfully acknowledge the media are doing" (2003: 224-5).

3.1.5 Generations five and six: The Microserfs and the free/libre and open source software (FLOSS) movement

Gisle Hannemyr (1997, 1998) introduces the idea that the methods and ethics of hacking are capable of generating software superior to that produced by the rigidly Taylorist methods of specialisation and standardisation that were commonplace in software engineering at the time. This positive perspective may seem surprising, given that Hannemyr is a Norwegian computer security officer.

3.1.5.1 Black hat / White hat

However, many 'compsec' or 'infosec' professionals consider themselves hackers, albeit 'ethical' ones, and hacker conferences or 'cons' such as the NZ Kiwicon or the US/global DEF CON ('DEF CON') pull together both 'black hat' (hackers who

break the law) and 'white hat' (ethical hackers or computer security professionals) participants, not to mention all the shades of 'grey hat' in between. The Kiwicon Wikipedia entry, which appears to have been written by involved parties (in that it is in the style of the text on the Kiwicon website – see Figure 1), gives a good account of the general atmosphere at a hacker con:

> Kiwicon provides a venue for hackers and computer security professionals as well as other interested parties to get together and share knowledge, war stories and to consume a startling amount of beer. In the spirits of DEF CON and Ruxcon, Kiwicon intends to bring together the best and brightest from academia, the computer security industry, the hacker underground, those who manage critical infrastructure and law enforcement.
>
> ('Kiwicon: Wikipedia')

Figure 2: The Kiwicon 2K7 website homepage[5]

This diversity of attendance was apparent at the conference, with the maxim of 'knowing your enemy' (and even having a beer with them) being strikingly apt.

[5] Image from: http://2007.kiwicon.org/

The distinction between black hat and white hat or ethical hackers, and the proportions of each at hacker cons was something one of the Kiwicon attendees, the CEO of Securus Global (an Australian/global computer security company), made comment on ('Securus Global'). When asked whether he classed the work he and his colleagues did as hacking, he replied:

> The "hacking" (ie; testing websites and access points for clients) is just a small part of what we do. We perform a raft of other activities whose goal is to help secure our client's environments […] Do we call the hacking part "hacking" ….yeah….it is what it is and our clients are happy to call the "tests" hacking / pen [penetration] tests. They want to know what hackers could do to them but we try to shut down these paths before they potentially impact our clients.
>
> (Drazic 2007a)

In relation to this, and in response to a question regarding the distinction between hacker and cracker, and the media's role in negatively defining the term 'hacker' for the general public, he also made it clear that he felt the media pathologisation of the term 'tainted' all Kiwicon attendees and hackers in general with suspicions and negative connotations, whether they deserved them or not:

> It's tough with the media sometimes because they like to sensationalise it. They would love to think and certainly like to allude to events like Kiwicon being full of rogue hackers. While some in attendance may fit that bill, most are not… just because you know IT well and can perform this work, there seems to be a grey cloud above those people.
>
> (Drazic 2007a)

Clearly, as evidenced by this statement, and in the previous self-descriptions of Kiwicon, hackers are most certainly not blind to their poor public reputation or the

media's role in this, with one of the organisers of Kiwicon also characterising media coverage of hacking as 'sensationalistic' (Metlstorm 2007a).

Returning to Hannemyr's argument, he compares 'hacker' and 'non-hacker' software, for example, the Linux OS vs. MS Windows, summarising that:

> …[s]oftware constructed by hackers seems to favour such properties as flexibility, tailorability, modularity and open-endedness to facilitate on-going experimentation. Software originating in the mainstream is characterised by the promise of control, completeness and immutability.
>
> (Hannemyr 1997)

These characteristics reflect the differing production environments, citing the benefits of an "agoristic, integrated and holistic attitude" as opposed to a "proprietary, fragmented and reductionist" one (ibid.). The Linux OS and the GNU project are cited as examples of the programming success the hacking approach can achieve, and he concludes that it should be considered, at the very least, as a complementary approach to Taylorism.

The concept of hacking as a work ethic had been previously touched upon by Turkle (1995), and Raymond (1999), and was extended in Himanen's (2001) *The Hacker Ethic: A Radical Approach to the Philosophy of Business.* None of these texts are worthy of further examination due to their excessively lyrical, subjective or glancing perspectives on hacking. Hannemyr's articles are also of limited current relevance, as feedback on this matter sought from various software engineering professionals indicates that their workplaces currently practise systems of production that incorporate exactly the hybridity that Hannemyr is suggesting. This merely recognises that Hannemyr's texts are perhaps somewhat dated (an inescapable reality in a rapidly evolving and relatively young industry) or idealistic, but far from invalid.

Indeed, Hannemyr's texts hint at the fifth and sixth generations of hacker identified by Jordan and Taylor (2004) – the Microserfs and the free/libre and open source software (FLOSS) movement. Microserfs may be broadly understood as hackers/computer programmers who have been co-opted by computer programming corporations such as Microsoft, thus 'selling out' on the hacker ethics of anti-bureaucracy, anti-authority and informational freedom. Presumably, ethical hackers or computer security professionals are also partially characterised by this category, although one suspects (from those spoken to) that this descriptor would not likely be well received.

Conversely, those involved in the FLOSS movement are hackers who have stayed true to these ethics, and instantiated them in the dispersed and collaborative production of free and/or open source software. Richard Stallman, the GNU Project and operating system (OS) and the associated GNU General Product Licence (GPL); the Free Software Foundation; Linus Torvalds, the Linux project, and particularly the Linux distribution Ubuntu OS, which now has an estimated user base of over 12 million (Kerner 2010); all are prominent examples and embodiments of the FLOSS movement and ethos. (The FLOSS movement is a fascinating evolutionary offshoot of hacking, and is worthy of much research in its own right, but will be dealt with only briefly here.)

Hannemyr effectively pits these two generations against one another in terms of both work ethic and productivity. As previously argued, the distributed, collaborative work ethic of the FLOSS movement (or of hacking as Hannemyr sees it) has also been co-opted to some extent by the corporate programming world, but there is no doubt that the informational freedom ethics of the two generations are well and truly in direct contrast. The four freedoms of the free software definition are as follows:

> Freedom 0: The freedom to run the program for any purpose,
>
> Freedom 1: The freedom to study how the program works, and change it to make it do what you wish,

> Freedom 2: The freedom to redistribute copies so you can help your neighbor,
>
> Freedom 3: The freedom to improve the program, and release your improvements (and modified versions in general) to the public, so that the whole community benefits.
>
> ('The Free Software Definition')

These clearly run in direct contravention to the proprietary ethos underpinning corporations such as Microsoft and Apple. The open source philosophy shares many of the same principles, although free software purists often look down upon open source as a development methodology as opposed to a social movement. "For the Open Source movement, non-free software is a suboptimal solution. For the Free Software movement, non-free software is a social problem and free software is the solution" ('Why "Free Software" is better than "Open Source"'). Nevertheless, both are anathema to proprietary, bureaucratically and hierarchically organised software development or 'Microserfdom'.

Hannemyr's texts also recognise the media's (by now well-established) role in hacking's gradual popular and legal criminalisation, and the contested nature of the terminology, with the author taking hacking as a set of ethics and open, anti-hierarchical labour methods, best embodied by Jordan and Taylor's sixth generation, the FLOSS movement.

3.1.6 Tim Jordan and Paul Taylor: A summarisation and extension of hacking and its generational evolution

The late Nineties also marked the beginning of Tim Jordan and Paul Taylor's extensive combined body of work on hacking, with their (1998) article, 'A Sociology of Hackers', refuting the popular perception of hackers as the

pathological "obsessed, isolated" (ibid.: 775) individuals of Chandler's (1996) third and fourth categories of media images. This pathologisation is allegedly reflective of a wider fear of computers and the unknown, which hinders any true understanding of hacking. They make their argument through a sociological investigation of hacking communities, drawing heavily on interviews with hackers. Initialising the article with a discussion of the terminology, they subscribe to the concept of hack described by Turkle (1984). A hack must demonstrate:

> 1) Simplicity: It must be simple but impressive,
>
> 2) Mastery: Despite its simplicity, the hack must derive from sophisticated technical expertise, and
>
> 3) Illicitness: The hack must be against some institutional, legal or even just perceived rules.
>
> (Turkle 1984: 236, in Jordan & Taylor 1998: 759)

This definition of the hack draws clear parallels with Levy's (1984) definition, additionally defining illicitness as more than a purely legal condition, interlinking with Levy's first, second and third ethical tenets. Given the hegemonic stabilisation of the capitalist ideology in the modern environment, a philosophy calling for unlimited (by price or artificial scarcity) access to and circulation of computing resources and information is certainly illicit in Turkle's sense, and a mistrust of and resistance to centralised authority is similarly 'against' the hierarchical power bases that govern both political and economic modern life.

The hack is further identified as an end in itself, and the more it is copied, the more diminished its status becomes – following a pre-hacked protocol will not garner hacker respect (Jordan & Taylor 1998: 760). By this stage, the Internet and World Wide Web were well established, with hackers and hacking embracing this expansion of the digital environment, and this text exists firmly within this context. This identification of the fundamental requirement of originality in the pursuit of hacker 'kudos' is a clear response to the rise of Internet-enabled 'script kiddie'

activity. A script kiddie is a term the hacker community use to describe someone who runs scripts or programmes written by someone else and distributed via the Internet in order to attack computer systems, rather than 'scripting' their own (Jordan & Taylor 2004: 8). Script kiddies may be seen as a debased subsection of the hacker/cracker generation, although many 'real' hackers would argue that script kiddies are not really worthy of being described as hackers at all.

3.1.6.1 The collective identity negotiation of hackers

Jordan & Taylor's sociological analysis of hacking communities addresses demographics, cultural aspects and external factors. No real demographic conclusions are drawn because of the confounding factors of anonymity, sample self-selection, and reticence founded on fears of prosecution. The data from the three surveys examined in an attempt to judge the size of the hacking community is inconclusive due to variable sample sizes, statistical methods and results. However, six cultural factors are extracted from the interviews with hackers, and hypothesised as providing internal community cohesion through collective identity negotiation. These factors are summarised below:

1) Technology: Hackers share an easy, innovative relationship with all technology, not just computers. True hackers hack anything and everything.

2) Secrecy: Hackers have an ambivalent relationship with secrecy. They keep their actions secret from authority but visible to their peers, in order to share information and garner recognition or kudos for their feats.

3) Anonymity: This factor is linked to secrecy, in that offline identities are kept secret while an online persona is actively constructed.

4) Membership Fluidity: Hacker communities are informal networks with high member turnover. This is due to the organic reasons of growing out of hacking and the massive commitment needed to remain 'up to date' in such a dynamically changing environment, but also because it makes detection and prosecution much more difficult.

5) Male Dominance: Little evidence of female hackers was found. This is linked to the fact that computer science is generally male dominated, through childhood socialisation factors and a masculine learning environment. The macho competitiveness of hacking and possibility of online misogyny fuelled by anonymity are also faulted, but no evidence provided sufficiently explains this gender anomaly.

6) Motivations: The motivations uncovered by Jordan and Taylor through their interviews were feelings of addiction and compulsion; curiosity; being online as an act of escapism from a boring offline existence; feelings of power; the desire for peer recognition and acceptance, and an altruistic desire to improve network security.

Several of these findings were corroborated by observations made at Kiwicon 2007 and through communication with attendees. There were very few women attendees at the conference, and many of them appeared to be the partners or friends of male hackers involved in organising the conference, and were helping out with administrative tasks such as staffing the door, and distributing tickets, programmes and lanyards. Out of the 16 presenters, none were women, and the Kiwicon organising team was self-described (albeit self-deprecatingly, in reference to a communication breakdown) as "a group of dudes" (Metlstorm 2007a). There was no obvious misogyny demonstrated, but a strong sense of aggressive competitiveness was present, with much heckling of presenters who botched aspects of their live demos, and even instances of audience members hacking into the live demos presenters were projecting onto the conference screen, and posting messages referring to the presenter being 'pwned' (hacker slang for taking control of/dominating/humiliating a target) and calling him names. The tone of all this

behaviour was light-hearted rather than truly malicious, but it did certainly fit the usual socially constructed notions of 'macho' as opposed to 'feminine' behaviour.

With regards to having an easy, innovative relationship with technology, Metlstorm's previously reproduced statement described hacking as:

> …an expression of curiosity and a desire to understand the operation of complex systems, in the same category as other enthusiasts.
>
> (Metlstorm 2007a)

This speaks to a wider engagement with complex systems (or technology) of multiple types, and clearly, all who presented demonstrated extremely advanced programming proficiency and knowledge of computing systems. Those spoken to identified a range of motivations behind their hacking, corroborating all those described by Jordan and Taylor, with the notable exception of 'feelings of addiction or compulsion', with many adding that another primary motivation for them was to get or keep/do a job (as a compsec professional).

Jordan and Taylor's third portal into the hacking community examines the manner in which they maintain their external boundary. This is done through an act of constitutive exclusion - an 'us vs. them' mentality that is maintained through their relationship with the computer security (compsec) industry. Given the significant cross-over evidenced in the New Zealand hacker community (or at least that portion of it attending Kiwicon), it is unclear how relevant or accurate this information is – perhaps it is just that it is slightly dated and from a different context – but the issues raised over online-offline crime analogies are worth mentioning. In Jordan and Taylor's interviews, the hackers are variously described by the compsec professionals interviewed as 'stupid kids', 'vermin', and 'vandals'; similarly, the hackers collectively described the compsec industry as being comprised of arrogant control freaks on a power trip (ibid.: 770).

However, it was acknowledged that some crossover occurred, with some hackers ending up working for the CSI and others involved in security testing, as previously outlined. The tendency for the compsec industry to draw analogies with physical crimes such as theft and breaking and entering, and the disfunctionality Jordan and Taylor identify within these analogies is significant, as physical crime analogies have been and still are consistently utilised in anti-hacking rhetoric and cybercrime legislation. As Jordan & Taylor explain, likening data theft to physical theft is flawed in that taking a digital artefact does not diminish the existence of the original copy, and breaking and entering or trespass as offline equivalences to hacking are also problematic, in that hackers frequently cause no damage, and sometimes even help the victim to identify a security flaw.

In summation, they define Levy's (1984) hacker ethic as an articulation of "the complex construction of a collective identity" (Jordan & Taylor 1998: 775). Despite their exclusive reliance upon the self-articulated reflections of hackers on hacking (hardly objective sources), their conclusions are valuable, especially given the 'imagined community' thrust of their argument. They mark the beginning of an impressive chain of literature from the duo, which makes significant headway into a sociological understanding of hacking.

Tim Jordan's (1999) *Cyberpower* does not focus exclusively on hackers, but on the wider subject of its title. Cyberpower is defined as "the patterns of social relations that create systems of domination, whose articulation in cyberspace fuels an even more dominant elite" (1999: 141). However, a brief discussion of hacking is undertaken. In Jordan's opinion, hackers can be "some of the most powerful inhabitants of cyberspace", despite many not having access to the latest and best in computing resources (ibid.: 90). He acknowledges that cost and access can be problems, but can also be "radically overestimated, particularly within developed countries" (ibid.). Expertise is seen as more of a barrier than cost, and hackers defined by being willing to put in the time and effort necessary to enable their equipment to take control of more powerful machines. The fact that hacking rarely requires a great deal of audiovisual computing resources, and the inexpensiveness

of satisfactory second-hand computers[6] are given as further reasons for the comparative irrelevance of possessing the latest tools.

> There are numerous examples of hackers using astonishingly outdated equipment to control the most powerful resources of cyberspace … Hackers demonstrate the extreme end of the technopower elite, where material resources are close to zero, though never actually zero, and expertise is monumental.
>
> (Jordan 1999: 139)

This point has been re-verified recently; the so-called 'Pentagon hacker', Gary McKinnon, committed what one prosecutor has called "the biggest military hack of all time" with a dial-up modem (Boyd, 2008), and although this status is debatable (Ruffin 2009a), McKinnon penetrated several supposedly secure military networks with what is generally regarded as outdated equipment. Jordan's observations are useful for tentatively situating hacking within wider patterns of socio-economic privilege, although he fails to really address the idea that hacking 'know-how' is stratified along similarly socio-economic lines.

Paul Taylor expands upon the sociological analysis of Jordan & Taylor (1998) with his (1999) volume, *Hackers: Crime in the Digital Sublime*. Similarly, this text relies heavily upon interviews conducted by the author with Dutch hackers, and is packed with quotes from interview transcripts. Taylor organises these in such a way as to support his main points, which are largely an extension of the hacker sociology he and Jordan previously proposed. The book is a rich source of insights into the hacking psyche, and a fascinating, accessible read that is likely to be enjoyed by the public and academia alike.

[6] This is seen as largely a result of Moore's law holding more or less true (Manners 1996, and Rafferty & Tran 1996, in Jordan 1999: 91): it states that processing power will double every eighteen months, which means that every eighteen months computer prices should accordingly have dropped by half, or that double the processing power should be available for the same price. Therefore, second-hand computers are cheap.

Taylor re-acknowledges the contestability and gradual criminalisation of the term, noting its currently accepted meaning as related to "the unauthorised access to and subsequent use of other people's computer systems" (1999: xi). He sees this as a result of "hyperbolic misrepresentation" (ibid.: xii) in the media, which is bound to the information revolution. As a society struggling to cope with the instability and generational discrepancies generated by rapid technical change and a world viewed in increasingly informational terms, hackers "serve to remind us of our technical vulnerability/ignorance" (ibid.: 1), with otherwise powerful groups particularly susceptible to fears that "their own apparent strength and superiority may prove to be an Achilles heel" (ibid., p. 8).[7] However, it is also acknowledged that hackers have a tendency to play up this mystification with their penchant for threatening pseudonyms and group monikers; e.g. The Legion of Doom, Bad Ass Motherfuckers, Toxic Shock, etc. (ibid.: 6). This tendency has been confirmed in this authors' own interactions with hackers – Metlstorm, Bogan and Headhntr were some of the typically hard-edged hacker 'handles' in evidence at Kiwicon, amongst many others.

Taylor again refers back to Levy (1984) and Turkle (1984) for their characterisations of the hack and hacker ethics, and proposes a further two generations, or 'second wave' be added to those of Levy (1984) – the previously mentioned hacker/crackers and Microserfs (who he names after Douglas Coupland's eponymous novel). As Taylor acknowledges, these generations are not discrete, but they are, nonetheless, a useful means of categorisation. This proposed categorisation is reformulated in 'Hackers: Microserfs or Cyberpunks?' (Taylor, 2000), with the author drawing upon fictional representations of hackers to bifurcate the fifth generation into "the empty regimented capitalism" of 'Microserfs' and the "anarchic individualism" of 'Cyberpunks'[8] (2000: 55) – a differentiation later

[7] An amusing example of this is given by Taylor (2000). In 1983, Robert Morris Senior, then Chief Scientist at the U.S. National Computer Security Centre, is on record as stating that "[t]he notion that we are raising a generation of children so technically sophisticated that they can outwit the best efforts of the security specialists of America's largest corporations and military is utter nonsense. I wish it were true. That would bode well for the technological future of the country" (Lundell 1989: 11, in Taylor 2000: 42). Five years later, his son, Robert Morris Junior created and unwittingly unleashed 'The Internet Worm', one of the first self-propagating computer viruses, which caused widespread destruction in large sections of the Internet and damages variously estimated at multiple millions of dollars.

[8] Cyberpunk is a genre of literary fiction, the most famous example being William Gibson's *Neuromancer*. Cyberpunk literature is often characterised by a narrative environment of constant

abandoned. The erosion of the original, anti-authoritarian hacker ethic into 'Microserfdom' is seen to result from hackers' interest in the intellectual thrills of hacking as an end in itself subsuming their interest in hacking as a means of political expression (Taylor 2001: 489).

Taylor (1999) reiterates the cultural aspects he sees as integral to the internal self-definition of hacking communities, adding youth to the list and providing a more thorough examination of hackers' overwhelming masculinity, though again acknowledging that socio-cultural and psychological factors still fall short of a comprehensive explanation (ibid.: 26-42). The reassessment of hacker motivations retains some of those given in Jordan & Taylor (1998), and two new motivations are also introduced: boredom with the formal computing education system, and political acts.

3.1.6.2 Hacking as an explicitly political act

Boredom as motivation is self-explanatory, but the identification of politically-motivated hacking is extremely relevant in terms of its antecedence to hacktivism proper (and its interpretation through a public sphere theoretical lens) and connection back to Levy's (1984) first three ethical tenets. According to Taylor, "[s]ome hackers claim that they are a principled force within society dedicated to opposing the re-establishment of traditional values in the newly emerging information society" (1999: 61). Specifically, they are opposed to what they see as the unjustified privatisation and commodification of information, and rather than demonising technological artefacts like many countercultures, "they prefer to use them to their fullest advantage" (ibid.: 62). This utilisation occurs through software production and computer systems intrusion that specifically targets information commodification and copyright enforcement. Metlstorm's identification of his opposition to digital rights management (DRM) tools and software patents as a

change, an addiction among its protagonists to transcending the 'prison of the flesh' via online avatars, and a tension between freedom and corporate cooption.

motivation for his hacking, in that they represent a 'threat to open computing' is exemplary of this perspective (2007b), as is the last portion of the answer to the 'What is a hacker?' question in the Kiwicon online FAQ:

> In a world where society's technological dependence is as obvious as the technology itself is opaque, hackers provide the tools and language for social conscience, balance and freedom.
>
> ('Kiwicon FAQ')

In a continuation of Taylor's work, Andrew Ross's 'Hacking Away at the Counterculture' (2000) examines the media discourse on hacking as a systematically constructed panic to defend the corporate agendas regarding intellectual property and copyright law, and to ensure the severest possible prosecution of apprehended hackers. Echoing the previously discussed literature, Ross states that "[a]n increasingly criminal connotation today has displaced the more innocuous, amateur-mischief-maker-cum-media-star role reserved for hackers until a few years ago", and sees the function of this demonisation as allowing property law to be rewritten "to contain the effects of the new information technologies" (2000: 250-251). In response to this, he presents a range of the most common defences of hacking, worth reproducing in full, that run from "the appeasement or accommodation of corporate interests to drawing up blueprints for cultural revolution:

> a) Hacking performs a benign industrial service of uncovering security deficiencies and design flaws.
>
> b) Hacking, as an experimental, free-form research activity, has been responsible for many of the most progressive developments in software development.
>
> c) Hacking, when not purely recreational, is an elite educational practice that reflects the ways in which the development of high technology has outpaced orthodox forms of institutional education.

> d) Hacking is an important form of watchdog counterresponse to the use of surveillance technology and data-gathering by the state, and to the increasingly monolithic communications power of giant corporations.
>
> e) Hacking, as guerrilla know-how, is essential to the task of maintaining fronts of global resistance and stocks of oppositional knowledge as a hedge against a technofascist future.
>
> (Ross 2000: 252)

The explicitly political nature of hacking, having run through the literature since Levy (1984), has clearly started to gather growing momentum and significance in a technological environment increasingly under corporate and governmental control.

Ross argues that the reason hacking is less positively associated with counter-cultural activity than, for example, the hippies, is that its counter-cultural side is harder to recognise due to the anonymous and covert nature of the activity. He refutes the dismissal of hackings' political significance as made by Dennis Hayes, who contended that "teenage hackers resemble an alienated shopping culture deprived of purchasing opportunities more than a terrorist network" (in Ross 2000: 259). Hacking's significance as one of these cultures lies less in its complex articulation of a political philosophy than in its "embryonic or *protopolitical* languages and technologies of opposition to dominant parent systems of rules" (ibid.: 259-60) (italics in original). This protopolitics, based on a belief in open access to computing technology and to knowledge and information, is evident in a statement made by Metlstorm in a response to a general question about hacker ethics or ideologies:

> Certainly a pretty reasonable proportion of people-with-hacker-powers are of an ideological bent, especially those of the older generation for whom access to information and computer systems was a motivation for learning.
>
> (Metlstorm 2007a)

Ross sees increasing digital surveillance – the digital panopticon – as a system of social management that promotes a siege mentality by cultivating the identification of omnipresent domination. Hacking is a siege breaker, critiquing existing technologies and cultural programmes while offering new alternatives, thus encouraging 'technoskepticism', which he sees as a necessary (though not sufficient) condition for social change (ibid.: 262-267). Ross is perhaps somewhat idealistic in his overall assessment of hacking, but he definitively articulates the inherent and potential political significance of hacking in an innovative and invaluable manner, while acknowledging the obscuration of this potential through corporate-sponsored media discourse.

The new millennium also brought the publication of Thomas's (2000) 'Criminality on the Electronic Frontier: Corporality and the Judicial Construction of the Hacker'. This deals primarily with the concepts of physicality and prosecution, arguing the inappropriateness of forcing physical standards of legality on a non-physical act. This argument has obvious connections with Duff & Gardiner (1996), and with the deflation of physical analogies for hacking as espoused by Jordan & Taylor (1998) and Taylor (1999). Thomas deconstructs the law enforcement discourse regarding hacking in terms of its constant reference to corporeality, situating the body as the "primary locus for the jurisdictional construction of the hacker" (2000: 34). He notes the norms of prosecuting hackers for their ownership of potentially illegal technology as opposed to their use of this technology, with "[t]he constitutive act of possession … transformed judicially into the performative act of hacking" (ibid.: 25); and of similarly prosecuting their unauthorised presence in computer systems rather than the actual harm effected. The non-corporeal criminal nature of hacking is unable to be dealt with by either the media or law creation/enforcement institutions, with:

> …outmoded standards of legality and characterisations of criminality … forced upon hackers. […] The discourse surrounding hacking reveals little about hackers themselves, but, instead, tells us a great deal about social attitudes to technology.
>
> (Thomas 2000: 35, 27)

Like Jordan and Taylor, Ross sees the general fear of hacking as reflective of a more general discomfort with technology – their 'easy relationship with technology' (Jordan & Taylor 1998; Taylor 1999) makes us uncomfortable about our own use of and reliance on technology, and hence, uncomfortable about our place in the world. However, like Jordan and Taylor, these intuitively valid hypotheses are not backed up with any real evidence, although admittedly, these kind of conceptual correlations would be difficult to support in an objective empirical fashion. Nor does Thomas suggest any alternative and superior philosophy of dealing with hacking in a legislative context.

3.1.7 The seventh generation: The emergence and identification of hacktivism proper

Paul Taylor's (2001) 'Hacktivism – In Search of Lost Ethics?' and (2004) 'Hacktivism: Resistance is Fertile?'; and Jordan & Taylor's (2004) *Hacktivism and Cyberwars* each reiterate the complicity of the media in fear mongering and criminalising the image of hackers. Taylor (2001) cites a characterisation of media reportage on hacking by (1) its obsession with hypotheses about what might have happened – the "standard nightmare scenario" (Sterling 1993: 40) mentioned previously – rather than what actually happened; (2) an abuse of anonymous sourcing and secrecy; and (3) paranoid gossip (Smith 2000, in Taylor 2001: 68-9). Jordan & Taylor (2004) again place this fear within the context of 'viral times', in which the communication systems of advanced capitalism have "created conditions that allow information to act in viral-like ways" (2004: 20). The public fear of hacking is thus a function of a wider vulnerability to viral information, due to the disconnect between our reliance upon networked technologies and our ability to maintain and control these technologies (ibid.: 21). Hackers are scapegoats for these feelings of vulnerability.

The media are also condemned for failing to differentiate between hackers and crackers. Crackers are defined as criminal hackers (ibid.: 4), highlighting yet again the contested terminology observable throughout the hacking literature. What exactly Jordan & Taylor's definition of 'criminal' constitutes is not made perfectly clear, but we might contend that it intends to differentiate those hackers who knowingly and intentionally cause malicious and ideologically aimless damage to the computer systems they have entered on an unauthorized basis. There is no real way of knowing their true lexical intention, but this is a useful interpretation to make.

Furthermore, each text again harks back to Levy (1984) and Turkle (1984) for their definitions of hacking, and their significant advance on the generations of hacking as previously proposed by Levy (1984) and Taylor (1999, 2000) is solidified in Jordan & Taylor (2004). Generations four, five, and six of this 'second wave' have been delineated previously, but are recapped below, with the additional seventh generation of hacktivism included.

> 4) Hacker/Cracker: This generation is seen as having emerged during the Eighties, and its members defined as those "who illicitly break[s] into other people's computer systems, though not always for malicious reasons" (2004: 11). 'Hacker' is acknowledged as the term in general usage, while 'cracker' is often used internally among the community to preserve the original meaning of 'hacker' (ibid.: 12).
>
> 5) Microserfs: "[C]omputer programmers who, while exhibiting various aspects of the hacker subculture, nevertheless have become co-opted into the structure of larger corporate entities, such as Microsoft" (ibid.), their "corporate-friendly hacker characteristics … harnessed to silicon capitalism" (Ross 1991: 90, in ibid.:15).
>
> 6) Open Source: "This community connected its concern for the individual hack to a disdain for 'bloated' commercial software and set in

chain processes for producing free, elegant (hopefully) and constantly peer-reviewed software" (ibid.:12).

7) Hacktivism: This is defined as "the merging of hacking activity with an overt political stance" (ibid.), and emerged during the Nineties.

The perceived ethical content of hacking peaked during Levy's (1984) first and second generations, fell during generations two through six (with Microserfs comprising "the nadir of the original hacker ethic" (Taylor 2001: 63)), and began to peak again with the rise of hacktivism (Taylor 2001: 61). The final two generations emerged as a backlash to the corporate cooption of hacking, and "mark a retreat from such a pervasive intrusion of commodified values into social life, and a concomitant reassertion of more countercultural values" (2004: 15-16). Jordan & Taylor again acknowledge that this schematisation is difficult because there are overlaps in time and ethics, as well as depictions of hacking being contested both within and without the hacker community (2004: 9-10),. As such, these generations are best understood in what might be best described as Foucauldian genealogical terms – they articulate the every-thickening discourse surrounding hacking (and, by extension, hacktivism) rather than providing any kind of strictly demarcated chronological evolution. Each new generation builds upon rather than replaces the previous one, generating an ever more dense and interlinked discursive field. Even though it is not chronologically accurate in any strict sense, this final realisation of the 'generations' of hacking is valuable in the overall trends and diffusions it identifies within the movement.

3.1.8 The increasing conflation of hacking and cybterterrorism

Jordan and Taylor also recognise the increasing media conflation of hacking and cyberterrorism, with cyberattacks often more hyped than fatal physical attacks

(ibid.: 26-28), an observation which leads us into the literature of Sandor Vegh. His (2003) doctoral thesis focuses (in part) on the change in public discourse concerning hacking and hacktivism before and after 9/11, investigating an increasing conflation with cyberterrorism as a recent evolution on the criminalising discourse on hacking, as hinted at by Jordan & Taylor (2004).

He begins by acknowledges the original non-computer-specific understanding of the hack, defining it as "a challenge to social or cultural norms and customs … usually serving the interests of the producers in society" (2003: 152). Understood in this sense, he identifies all hacks as counterhegemonic, in that they break or overcome 'functional fixations' – limitations in artifacts "imposed by social conventions rather than original design" (ibid.: 152-3). Elite forces therefore obviously wish to constrain this deviance, especially since hacking "attacks data, the dominant property of the information age. The corporation's two greatest fears are revenue losses and deterioration of public image, exactly what a hack can bring about…" (ibid.: 153). He sees the media's role in demonising hacking as resulting primarily from a concerted indoctrination effort on the part of the combined forces of corporations and the American government, attempting to simultaneously control hacking and effect legislation supporting their own agendas. This will be discussed further in the next section, but it marks an intensification of the perceived purposiveness of the media fear mongering noted in previous literature.

Vegh also corroborates previous findings regarding the near-impossibility of accurately compiling meaningful statistics on hacking attacks, citing a document recommending sentencing guidelines for American courts. This document, signed by Stanford University's Centre for Internet and Society, the Electronic Frontier Foundation, and the National Association of Criminal Defence Lawyers, notes that individuals convicted of computer crime tend to receive far harsher punishment than those convicted of comparable offline crimes, and that they are generally punished according to the worst-case scenario rather than what they actually do (Granick et al 2000, in Vegh 2003: 210). The proposed post-9/11 Cyber Security Enhancement Act is also provided as evidence of this legislative tendency (ibid.: 208). The initial unamended Act proposal would have lumped most hacks in with terrorism,

rendering them prosecutable in the same secretive, unmonitored manner and punishable by life imprisonment.

The relevant literature on hacking concludes with Helen Nissenbaum's (2004) 'Hackers and the Contested Ontology of Cyberspace'. Her analysis of the mediated image of hacking parallels that of Vegh, in that she sees its shift toward negativity not only as a function of the sensationalist media, but the result of "an ontological shift mediated by the supportive agents of key societal institutions: legislative bodies, the courts and the popular media" (Nissenbaum 2004: 195). She contends that the government and private sector consciously demonise hackers, constructing them as a new, post-Cold War enemy and justifying their harsh punishment. In doing so, these elite sectors both retain control of normative ideology in a changing techno-social environment – the hackers are 'bad', examples of what not to be – and can justify further defence, security and law enforcement expenditure, as well as generally tightening their control on the free and open exchange of information (ibid.: 2000).

The corporate and regulative normalization of the Internet, contributing to the transformation of a "relatively intimate and mildly anarchistic environment to one governed by institutionally-imposed order" is a "sea-change" that has "stranded" hackers (ibid.: 202). In the new social ontology of cyberspace, hackers' status is as "agents who willfully defy the rules" (ibid.: 203), with Nissenbaum citing Bowker & Star (1999) and Boyle (1997) as corroboration of the potential political power of 'naming' or classification. This phenomenon of the world shifting around hacking was also described by the CEO of Securus Global:

> …what was once fun and and less open to someone getting in trouble is now a crime that could see you in jail for 20 years. There's been quite a few stories in the press. So what does a local hacker do? Most are decent people having fun so they stop the illegal part of their work and try to turn that skill into "research". Some continue. I would estimate 10%.
>
> (Drazic 2007a)

In this environment, not only is hacking legislatively criminalised, but the public is no longer in possession of even the vocabulary needed to conceive of the original, 'good' meaning of hacker. One need only contrast the literature on hacking with the coverage given to the activity in the mainstream media to recognise the truth in this statement. In any given news article, the hacker/cracker generation is likely to stand in for hackers in general, and only hackers and those studying hackers have access to knowledge of the incredibly polysemous nature of the term and practice. The FLOSS movement has gone some way towards reclaiming hackers' power to name themselves, but the mass mediated definition appears to be the victorious hegemonic project. Nissenbaum's hypothesis is founded upon a simple recognition of institutional resource superiority in influencing the media's construction of reality, hence 'reality' reflects the media viewpoint rather than that of under-resourced opposition movements.

3.1.9 Conclusion

This review of the literature concerning hacking provides an explication of the history, terminology, ethics and various perceptions of the practice, as well as illustrating the contested and constantly evolving nature of many of its components. From a non-specific initial application, hacking has become firmly entrenched within the technological, networked context of our times – within "the social structure resulting from the interaction between the new technological paradigm and social organisation at large" - what Manuel Castells terms 'the network society' (2005: 3). If we accept Castells' persuasive assertion that networks have become the basic units of modern society, and that real power is now located within these networks rather than within traditional geographically-bounded power hubs, then the ease and skill with which hackers navigate and manipulate these networked spaces of modernity lends them considerable advantages within this global mode of society. If indeed "nowadays wealth, power, and knowledge generation are largely dependent on the ability to organize society to reap the benefits of the new

technological system, rooted in microelectronics, computing, and digital communication" (ibid.), then hackers possess considerable latent and actual social, cultural and economic, but also political power. Politics is now "largely dependent on the public space of socialize communication [therefore] the political process is transformed under the conditions of the culture of real virtuality. Political opinions, and political behaviour are formed in the space of communication" (ibid.: 14). As we shall see, hacktivists are particularly attuned to this facet of the information or network society in which we now live, and this sensitivity, combined with their ability to manipulate these spaces of communication, means that they are increasingly puissant players in the game of networked global politics.

As such, the range of societal powers hackers possess is threatening to the status quo of established interests (particularly political-economic interests), and hackers have experienced ongoing image management issues in relation to this. These issues have been exacerbated by the floating polysemy of the terms hacker and hacking, which has left hackers vulnerable to attempts at external meaning making and fixing. Governments and corporate media often frame them as purely criminals or terrorists, conflating the term with the practices of cracking and cyberterrorism. These illegal and destructive practices are arguably best understood as a specific subsection of the increasingly dense discursive field surrounding computer hacking, but they are not representative of the practice at large. The programmers 'hacking up' code for money or love, for proprietary or free/open source projects, at work, at home, and in hackspaces, and the 'ethical hackers' or computer security professionals, are all hackers. They almost certainly comprise the vast bulk of the global hacker community in terms of sheer numbers. They are simply not as 'newsworthy' as those hacking into a power plant's SCADA[9] system or a bank's credit card records, or into Google, Adobe or Intel's corporate network to steal intellectual property.

It is clear that hacking, as a philosophy and practice, has been anti-authoritarian and countercultural from the outset, with this fundamental ideological vein guiding its eventual expansion into a more overtly political form; hacktivism. Building upon

[9] SCADA (Supervisory Control and Data Acquisition) systems are industrial control systems used to monitor and control processes within large power, water, manufacturing, transport or communication facilities or infrastructures, such as power plants and airports.

the foundation of hacking, the phenomenon of hacktivism as first introduced by Taylor (2001) will be investigated, placing it within both the recently constructed context of hacking, and that of the wider repertoire of 'electronic contention' (Costanza-Chock 2001). Its differentiation from this wider repertoire will be addressed, as will attempts to categorise its varying internal threads.

Chapter 4

Hacktivism: The revival and extension of the political ideology within hacking

> Hacktivism is something, in my opinion, that we've not really seen in action yet. It's one of those lurking things we know can be used to great effect, but hasn't really yet been exploited to it's full power.
>
> (Metlstorm 2007)

The previous chapter on hacking has provided us with a rich context for the ensuing review of hacktivism. Like, hacking, hacktivism is also a diverse practice, but, as a subgroup or evolutionary offshoot of hacking proper, can be defined somewhat more precisely. A review of the literature on hacktivism, grounded with examples, and further supplemented with excerpts from interviews and personal communication with organisers and attendees of Kiwicon, will establish a holistic understanding of the evolution, context and nature of the practice. This review will also assess various proposed models for an internal division or categorisation of hacktivism, and will establish the need for a public sphere theoretical treatment of the practice.

We have heard one description of hacktivism previously, from Jordan & Taylor (2004), who identify it as a trend emerging from hacking during the Nineties, and define it as "the merging of hacking activity with an overt political stance" (2004: 12). The conciseness and general thrust of this definition were echoed in definitions offered by two of the organisers of Kiwicon, who described hacktivism as below:

> Hacking for a political cause.
>
> (Bogan 2007)

> [The] [u]se of hacking techniques for politically motivated goals.
>
> (Metlstorm 2007a)

A comprehensive appraisal of the literature on hacktivism will extend upon this understanding, linking it firmly to the previous literature and knowledge on hacking, and to the wider contexts of online activism and an increasingly informational society. Various trends within hacktivism will also be identified.

4.1 The imaginary hacktivist

Curiously enough, the first texts on hacktivism worth assessing address it in a purely theoretical or hypothetical sense. Certainly, politically motivated web site defacements had already occurred, and hacking itself can be considered a form of political expression, as we have seen. However, these texts consider the additional possibility of less discrete, more systematic, communal, and creative applications of hacking practice for explicitly political ends – phenomena that had not yet occurred.

4.1.1 Hacktivism and Netwar

The first of these texts is John Arquilla and David Ronfeldt's (1993) 'Cyberwar is Coming!', published in the defence journal *Comparative Strategy*. It is perhaps not surprising that the possibility of hacktivism was first identified by members of the elite institutional network potentially threatened by it, rather than by academia. Indeed, the knowledge of hacktivism appears to have diffused right through into the news media before any non-activist or non-military-aligned/consulted academics took an interest in it. Arquilla and Ronfeldt's article is a rethinking of the theory

and practice of warfare and conflict, and the significance of knowledge in these emergent modes of conflict. They argue that "[i]nformation is becoming a strategic resource that may prove as valuable and influential in the post-industrial era as capital and labour have been in the industrial age" (1993: 24-5).

In line with this, they conceive of the rise in prominence of two forms of networked, informationally grounded conflict: 'Cyberwar' and 'Netwar'. Cyberwar is the main concern of their article, and is an exclusively military-level affair, but their peripheral concept of Netwar arguably includes the first rough theorisation of hacktivism. It is defined as (probably) non-violent "information-related conflict at a grand level between nations or societies", targeted primarily at information or communication systems:

> It means trying to disrupt, damage, or modify what a target population "knows" or thinks it knows about itself and the world around it. A netwar may focus on public or elite opinion, or both. It may involve public diplomacy measures, propaganda, and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote a dissident or opposition movements across computer networks.
>
> (Arquilla & Ronfeldt 1993: 28-29)

The practice of hacktivism incorporates several of these strategies. Arquilla and Ronfeldt conclude that networks can defeat institutions, and, as such, networked forms of opposition may require networked responses, warning that "[t]he future may belong to whoever masters the network form" (ibid.: 40). As one of the organisers of Kiwicon put it:

> As is often discussed in information warfare texts, the network is a multiplier – you can be instantly anywhere on the virtual battlefield,

> communicate seamlessly, and the scale of your attack isn't limited by the size of your force.
>
> (Metlstorm 2007a)

This article is only a vague intimation of the potential occurrence of hacktivist practices, and does not differentiate them from a wider subset of non-military, networked conflict strategies. Nor is the scope of the word "grand' explained, but it seems from this and from the war terminology that that the authors were thinking along the lines of strategic and ongoing multi-participant engagement. Hacktivism is not confined to this form. Nonetheless, 'Cyberwar is Coming!' is worth acknowledging for its prescience and the direction from which this prescience came.

4.1.2 The Critical Arts Ensemble and electronic civil disobedience

The next set of literature on hacktivism came from an almost diametrically opposed direction – the "broad based artist as activist collective" founded in 1986 and known as the Critical Arts Ensemble (CAE). The group of six core members is at least semi-academic: appearing regularly on the art and academic circuit; publishing regularly in art journals; producing several publications; and creating "[s]ituationist-style performances, street theatre and other disturbance 'art'" (Liu 2004: 361). Their art and literature is firmly and knowledgably grounded in postmodern theory, such as that of Deleuze & Guattari, Foucault, Baudrillard and Debord, with their methods proceeding on "the basis of a primarily Deleuzean critique of the social, economic, political and military powers of dominance" (ibid.).

CAE's contribution to the discourse on hacktivism began with *The Critical Disturbance* (1994), a collection of essays. One of the critical observations of this collection is that the forces of global dominance no longer reside in physical

locations, but exhibit 'rhizomatic mobility', using the instantaneous world flow of capital as their new instrument of domination:

> Elite power, having rid itself of its national and urban bases to wander in absence on the electronic pathways, can no longer be disrupted by strategies predicated upon the contestation of sedentary forces. The architectural monuments of power are hollow and empty, and function now only as bunkers for the complicit and those who acquiesce. They are secure places revealing mere traces of power… These places can be occupied, but to do so will not disrupt the nomadic flow.
>
> (CAE 1994: 23)

As such, CAE urge the transferal of resistance to the new virtual geography of cyberspace, proposing the 'electronification' of traditional methods of civil disobedience. They envisage a small group of hackers covertly bringing the "destructive force of inertia into the nomadic realm" (ibid.: 25) by disrupting or blocking the command and control of information, just as traditional protesters create blockages or disruptions in physical space. However, at the time of writing, they acknowledge that this is a purely fictitious scenario. The hacking community is seen as too apolitical and fragmented, with their 'free information' ethic in opposition to the disruption of the structures of cyberspace. Perceiving futility in asking them to "destabilize or crash [their] own world"(ibid.: 26), CAE encourage artist-activists to take up the mantle and encourage "speculation on a model of resistance within emerging techno-culture" (ibid.: 27), before electronic power relations are fully solidified and "we are left with only critique as a weapon" (ibid.). (This differentiation between politicised hackers and, for lack of a better word, 'hackerised' activists, is prescient in that it identifies a future actual schism within hacktivism.) However, they pessimistically conclude that when "[c]onsidering the history of utopia in ruins, the probability that this opportunity will be successfully used looks discouraging" (ibid.: 125).

CAE extend this discourse in *Electronic Civil Disobedience and Other Unpopular Ideas* (1996), exhorting activists to comprehend that the streets are "dead capital":

> Nothing of value to the power elite can be found on the streets, nor does this class need control of the streets to efficiently run and maintain state institutions. For C[ivil] D[isobedience] to have any meaningful effect, the resisters must appropriate something of value to the state.
>
> (CAE 1996: 11)

This is information, with its blockage and disruption striking most effectively at the core on the institution. This hypothetical new form of civil disobedience (CD) gives the book its title: Electronic Civil Disobedience (ECD). This term is one that is later sometimes conflated with hacktivism as a broader set of practices, but the distinctions between the terms and their individual relevance will be teased out through the subsequent literature.

An important point of note here is that although the CAE are arguably correct in identifying information as having become the most valuable political-economic resource (as opposed to the concrete artifacts of 'the street'), they go too far in classifying the streets as entirely 'dead capital'. There is, of course, still much value to be found in traditional street-based protest, as the 2010 New Zealand anti-mining protest and any number of constantly-occurring overseas protests show. Furthermore, the nexus between the streets and the internet is also proving immensely valuable, with most online protests incorporating some form of offline dimension, and many offline protests relying on web technologies for organisation and co-ordination.

Nonetheless, the CAE's call for activism to move to the electronic pathways is an important one (provided we avoid their extremist denial of the power of protest in the offline world), and they identify the schism between hackers and activists as the primary obstacle to the realisation of their vision. Because hacking is an extremely time-consuming form of constant self-education, hackers have little time left for politics, and tend to stay within their own community, hence, the opportunity for

hackers and activists to socialise is rare. Activists are lacking in the technical knowledge to effect ECD (ibid.: 19-20), hence "the schism between knowledge and technical skill has to be closed, to eliminate the prejudices held by each side (hacker intolerance for the technologically impaired, and activist intolerance for those who are not politically correct)" (ibid.: 20). (Oddly enough, it turns out that hacker intolerance for activist 'digital incorrectness' is more of a problem, as we shall see in section 5.4.3).

Drawing on negatively fraught media representations of hacking, CAE also posit that ECD will be demonised, conflated with malicious computer criminality without regard for motive, identifying the reasoning for this and their counter-argument as below:

> While the computer criminal seeks profit from actions that damage an individual, the person involved in electronic resistance only attacks institutions…Conflating electronic civil disobedience (ECD) with criminal acts makes it possible to seal off cyberspace from resistant political activity. Attacks in cyberspace will carry penalties equivalent to those merited by violent attacks in physical space…The same legal penalties that apply to CD should also apply to ECD.
>
> (CAE 1996: 17-18)

Some might argue that the literature of CAE is irrelevant; its authors lacking institutional academic status and their writing too subjective, rhetorical and hypothetical to be of any real use. However, their identification of the possibilities inherent in the convergence of hacking and activism is remarkably insightful. Furthermore, there is a strong argument for it having actually inspired its own realisation, in some instances at least. Finally, their prediction that ECD would be institutionally conflated with computer crime is yet another indicator of the perceptiveness of these texts.

4.2 The emergence of a hacktivist reality

One of the groups arguably inspired by CAE, the Electronic Disturbance Theatre (EDT), assembled over the next few years. Co-founded by one-time CAE member Ricardo Dominguez, it consists of four core artist-activists who consolidated in support of the Zapatista rebellion in the Chiapas region of Mexico. They began holding 'virtual sit-ins' in 1998, operationalising ECD as envisaged by CAE. A virtual sit-in can take a number of forms, with the most common based on page reload requests, but all have the intention of overloading a target server with an inundation of electronic information, thus effecting system/network slowness or a total crash. The EDT initially achieved their sit-ins manually, organising a collective pushing of the page reload icons on browsers targeted at a particular site. This progressed into the development of the FloodNet Tactical System (FloodNet) or the Swarm, software that automates the process (see Figure 2, next page). Zapatista supporters downloaded this software, and instituted several simultaneous attacks on a variety of Mexican and U.S. sites aligned with the Mexican government. An attack on September 9, 1998, was particularly noteworthy. Websites belonging to the Mexican President Zedillo, the Frankfurt Stock Exchange and the Pentagon all reportedly received 600,000 hits per minute. The Pentagon rather controversially fought back by redirecting FloodNet users to a site containing a JavaScript Applet ('HostileApplet') that overwhelmed the browsers of the estimated 10,000 protesters.

Dominguez and the EDT are still together and still engaged in hacktivist activity – their most recent project, the 'Transborder Immigrant Tool' utilises cellphone-based GPS technology to direct illegal Mexican immigrants to safe routes, shelter, food, water, and sympathizers during their attempted border crossings ('Transborder Immigrant Tool'). Unsurprisingly, this project has attracted a lot of criticism, and Dominguez, now an Associate Professor of Visual Arts at the University of California, San Diego, is, as of early 2010, facing criminal action and calls for the revocation of his tenure.

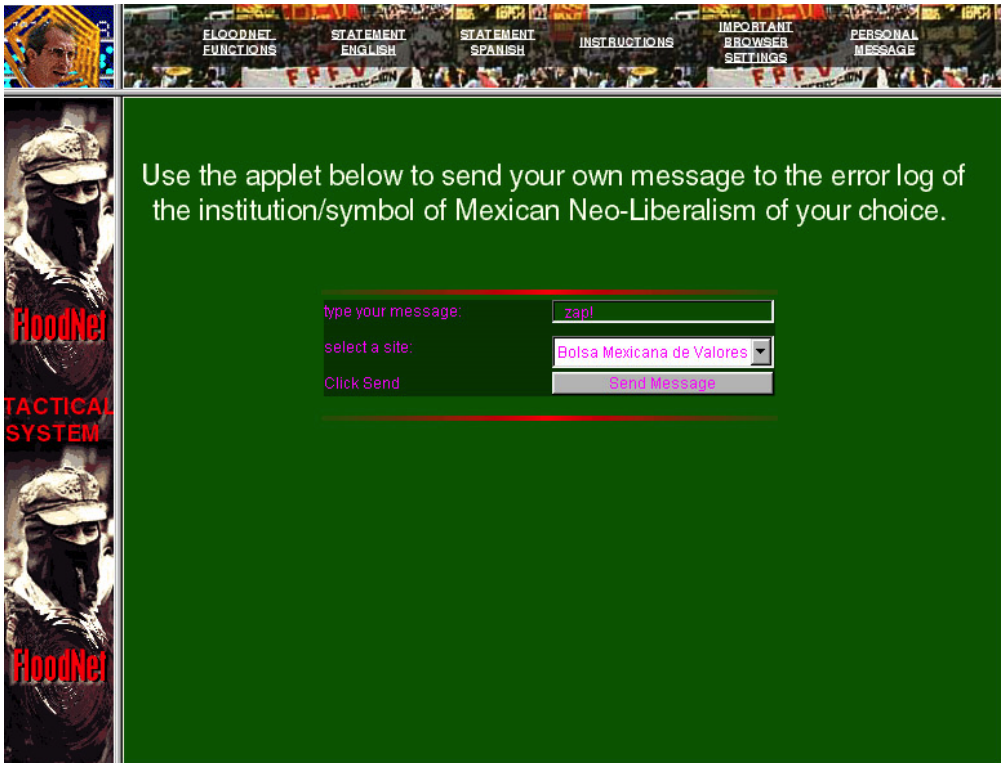

Figure 3: The FloodNet user interface (in Netscape)[10]

Tactics such as these and different hacktivist organisations will be gone into in more detail as required, but the main point to be grasped here is that 1998 marked the growing recognition of hacktivism as a reality. There were reports of 'hacktivity' on almost every continent (Wray 1998) and the New York Times published a front-page article (Harman 1998), thus inserting it into pubic discourse. This partially purposive garnering of media interest was, however, in direct opposition to the covertness advocated by CAE.

Another co-founder of the EDT and a then-postgraduate student, Stephan Wray, published 'Electronic Civil Disobedience and the World Wide Web of Hacktivism' in the same year. Wray proposes five portals for consideration, originally into hacktivism, but then thinks better of using the term and defines them instead as gateways into "the wider world of extraparliamentarian direct action Net politics" (Wray 1998), although he slips back into using the term 'hacktivism' later in the article. This inconsistency is the major flaw in an otherwise clearly executed

[10] Image from: http://trasescena.files.wordpress.com/2008/09/zapatista-tactical-floodnet.jpg

discussion; as seen in the discussion of hacking, naming and categorization can be powerfully significant acts, and providing a consistent terminological framework is privileged in academia. Nonetheless, Wray's article is important as it marks the first attempt to demarcate hacktivism both internally, and from the wider context of online activism.

The first of these portals, 'Computerised Activism', is "the use of the Internet infrastructure as a means for activists to communicate with one another, across international borders or not" – a practice correctly identified as having been in existence since the mid-Eighties, but having remained marginal until the "explosion of the Internet" and the World Wide Web in the early-to-mid-Nineties (ibid.). The next portal, 'Grassroots Infowar', is an intensification of the first, describing a shift beyond activists merely sharing information towards the incitement and organisation of real world action. From there, the intensity is wound up yet again, with 'ECD" and then 'Politicised Hacking'.

ECD is as theorized by CAE and applied by the EDT, and is defined as using "the Internet infrastructure as both a means for communication and a site for direct action" (ibid.). Politicised Hacking is the practice of web site defacements for explicitly political motives, which Wray acknowledges is not a strictly recent (circa-1998) phenomenon. It is differentiated from ECD by its methods, but also by the fact that it tends to be an anonymous, individual activity, as opposed to the public, collective nature of ECD – primarily because it is much more unequivocally illegal. Wray's final portal is 'Resistance to Future War'; a hypothetical utilization of all the previous tactics in a generalized resistance, such as was present regarding the Vietnam or Gulf Wars, but computer-assisted.

He closes with an assessment of the effectiveness and appropriateness of these techniques, now referring to them collectively as hacktivism in contradiction to his initial statement regarding the term. His assessment encompasses political, legal, tactical, technical and ethical factors; central issues raised are that hacktivism is likely to be supplementary or complementary to offline activism – a way to garner publicity but perhaps not likely to swell "the ranks of the disaffected" (ibid.). He also notes the potential that there will be disagreements over the appropriateness of disrupting bandwidth amongst otherwise politically cohesive groups, echoing the

internal schisms suspected by the CAE, but more correctly identifying their provenance. Nonetheless, Wray feels sure that hacktivism is on the rise, and is likely to continue to gain attention.

4.3 The conflation of hacktivism and cyberterrorism: Hacktivism's inheritance of hacking's image problems, pre-9/11

Dorothy E. Denning's (2000) 'Hacktivism: An Emerging Threat to Diplomacy' marks another contribution to the discourse from a defensive standpoint. Hacktivism, according to Denning is "not benign, and it threatens US Embassy computers and diplomatic missions. It can compromise sensitive or classified information and sabotage or disrupt operations. At the very least, it can be an embarrassment to those attacked and erode public confidence in the U.S. government" (Denning, 2000). No real advances in terminology or categorization are made; indeed, Denning's article is largely an account of various website defacements and automated Distributed Denial of Service (DDoS) attacks, and alarmist statements to the effect that things could have been and probably will become much worse.

Automated or server-side DDoS attacks occur when a hacker illicitly gains control of a network of computers (often referred to as a botnet) and uses them to wage an individually or multi-individually controlled, automated version of a virtual sit-in. The botnet is generally comprised of appropriated computers (bots), and usually established with trojans or viruses proper. Trojans are programmes disguised as something else, e.g. an email attachment, that self-install and either attack the victim computer or establish remote access for their creator/distributor. Automated/server-side DDoS attacks are different from virtual sit-ins because there is no collective element to their deployment. Virtual sit-ins may also be referred to as client-side or ethical DDoS attacks. The various usages of these terms differ from source to source, but we will persist with the usages already expressed, i.e. we

will use ‘DDoS attack’ to refer to server-side DDoS attacks, and ‘virtual sit-in’ to refer to client-side DDoS attacks.

Denning’s examples include the June 1998 anti-nuclear defacements and alleged data theft and destruction enacted by an international group of hackers referring to themselves as Milw0rm, against India’s Bhabha Atomic Research Centre; the site defacements relating to the 1999 Kosovo conflict and accidental bombing of the Chinese Embassy in Belgrade by NATO forces; and the simultaneous and massive server-side DDoS attacks on various commercial web sites, including Amazon.com, Yahoo.com, eBay.com and CNN.com in February 2000.

Amongst Americans, Dutch and Britons, it may interest local readers that New Zealand hackers were apparently part of the mix of hackers involved in the Bhabha hack. There was also a NZ connection in the 1989 WANK (Worms Against Nuclear Killers) worm incident, in which US Department of Energy and NASA computers all over the world were infected with a worm which changed their login screens to display a message informing the user that their system had “officially been WANKed”, and accusing them of talking of times of peace for all but preparing for war. In a nod to New Zealand’s nuclear-free status, the worm code contained specific instructions informing it to avoid New Zealand computers (Assange, 2006)[11].

Denning concludes that “[h]acktivism poses a genuine threat to U.S. government operations, particularly abroad”, but that so far as defensive tactics go, it can be lumped in with any type of cyberattack. These tactics are fundamentally run-of-the-mill security measures and processes that one would hope most personal computer owners, let alone governmental institutions, would practise. However, the real importance is in Denning’s casual grouping of hacktivism with all other cyberattacks. One gets the distinct impression that it is not seen as so very far from cyberterrorism, despite the fact that hacktivism was and is generally understood to exclude actions resulting in the public suffering physical harm or fatalities.

[11] Perhaps just as interestingly, the author cited here is Julian Assange, now director of Wikileaks.com, who started life as one of Australia’s most prominent hackers.

This increasing conflation with cyberterrorism is addressed by Manion & Goodrum (2000) in 'Terrorism or Civil Disobedience: Toward a Hacktivist Ethic'. They define hacktivism as "the (sometimes) clandestine use of computer hacking to help advance political causes" (2000: 14). It confronts both the corporate commodification of information and the violation of human rights, thus posing a threat at both the "private industry/intellectual property level and the national governmental/national security level" (ibid.). Their article's intent is to establish whether or not hacking activity can "reasonably be defined as an act of civil disobedience" (ibid.: 15), in line with the discourse of CAE and EDT. The principles determined as core to this definition are that the 'hacktions' must not be for personal profit, be demonstrably ethically motivated, and not result in human, financial or infrastructural casualties. Their essential recommendation is to assess each hacktion on a case-by-case basis, but that overall, hacktivism is a form of CD and therefore is ECD.

4.3.1 Electronic civil disobedience or hacktivism?

Like Wray (1999), Manion and Goodrum's terminology is somewhat confused, as web site defacements, which they mention, are not particularly analogous to the CD tactics of blockage and disruption. Graffiti or culture-jamming are surely more appropriate analogies. Furthermore, CD is almost exclusively a collective action, which website defacements rarely are. Defacements or DDoS attacks, however, may involve a single individual (or a small group of individuals) temporarily rendering a website unavailable or replacing its usual content, unlike virtual sit-ins, which attempt to harness the power of collective mobilization. Obviously, the differentiation is not incontrovertible[12], nor is it attempting to judge defacements as 'bad'; it simply aims to dispute the suitability of terming them ECD, and to argue that ECD is but a subset of hacktivist actions.

[12] Indeed, much defacement appears to be the work of two or more hackers. Furthermore, there is often no way to know how large a support group is behind any one defacement or DDoS attack.

Nevertheless, Manion & Goodrum's assertion that hacktivism is being conflated with cyberterrorism rather than considered in terms of its motivations and extremity of effect, with significant repercussions for both its image and the punishment of its practitioners, is of value. They see this as a purposive strategy on the part of governmental and corporate institutions to control copyright issues, legitimate the erosion of property rights and ignore a larger critique of information ownership and Internet commercialization (ibid.: 17). Defining hacktivism as a form of CD is integral to ensuring punishments that are in line with CD rather than with terrorism, and to allowing its continued practice as a critique of 'techno-control'. Despite Manion & Goodrum's use of the term CD, these sentiments are fundamentally sound, though as previously, no data is provided to support these allegations.

The following year saw further publications by Arquilla, Ronfeldt and Denning, all as part of a report, edited by Arquilla and Ronfeldt, and entitled *Networks and Netwars: The Future of Terror, Crime, and Militancy.* Sponsored by the American Office of the Secretary of Defence and conducted in the military think-tank RAND (National Defence Research Institute), its research perspective is predictable. Arquilla and Ronfeldt expand on their concept of Netwar, generously differentiating between its 'dark side' of "terrorists, criminals, and ethnonationalist extremists" and 'light side' of "civil-society activists" (Arquilla & Ronfeldt 2001: ix). The impression is given that the 'brighter' face is, in itself, still not particularly desirable, but has "positive potential if it can be harnessed" (ibid.: x). It is not precisely clear on which side of the coin hacktivism lies – Denning's chapter on it is in the 'light' section of the book, although her discussion ranges through to cyberterrorism, and the editors' note further muddies the waters[13] – and how exactly civil society activists who might be opposing aspects of the current American regime might be 'harnessed' to positive effect is somewhat mystifying. Their intentions appear to be good, but their tone comes across as rather patronising. One can almost hear them congratulating themselves for their munificence towards the activist universe.

[13] "Hacktivists and Cyberterrorists have not posed much of a threat to date, but this could change if they acquire better tools, techniques, and methods of organisation, and if cyberdefences do not keep pace." (Arquilla & Ronfeldt in Denning 2001: 239)

Their deconstruction of Netwar into five levels of theory and practice; technological, organisational, social, doctrinal, and narrative level, is valid if not particularly innovative. Similarly, their identification of 'swarming' (sustained series of attack pulses on centralised target/s by decentralised network cells (ibid.: 12)) as the key doctrinal approach to watch out for is also relevant, if borrowing rather heavily from the idea of smart/flash mobs. Various other refinements are made to their initial model of Netwar, but none are particularly useful in terms of hacktivism.

However, Denning's chapter is rather more useful. She conceptualizes a continuum of online protest much like Wray (1998), but culminates in cyberterrorism rather than a combination of the previous practices. The continuum runs from activism, to hacktivism, to cyberterrorism, with the boundaries between the categories defined as "fuzzy". Hacktivism is defined as "the marriage of hacking and activism", and covers "operations that use hacking techniques against a target's Internet site with the intent of disrupting normal operations but not causing serious damage" (Denning 2001: 241).

It is split into four categories; virtual sit-ins and blockades; email bombs; web hacks and computer break-ins (including site defacements, site redirects, and data theft or destruction); and computer viruses and worms. Email bombs are an attempt to overwhelm a target server with an automated flood of email messages, usually bearing some political message; and the basic difference between viruses and worms is that worms autonomously self-propagate whereas viruses are attached to files or segments of code, using their movements as a vehicle for distribution. However, due to evolution in their levels of sophistication, this difference is becoming less and less relevant. These are semi-valid divisions, but email bombs are a form of blockade and do not really merit their own category, as Denning herself admits.

Cyberterrorism is "the convergence of cyberspace and terrorism. It covers politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage" (ibid.). Denning's concern is that the tools of hacktivism can just as easily be the tools of cyberterrorism (ibid.: 280), and sees activism as the most effective means of protest, presumably because it is less likely

to be demonised by institutions acting on the inflammatory advice of consultants such as herself. What needs to be remembered with relation to all this discourse about the looming threat of cyberterrorism and semi-inclusion via proximal mention of hacktivism is that firstly, it was purely hypothetical in 2001 (see Vegh 2003), and is arguably still hypothetical now, depending on which definition of terrorism is utilised.

The 1975 USA Taskforce on Disorders and Terrorism (run by National Advisory Committee on Criminal Justice Standards and Goals) classified terrorism into six categories, one of which was 'Official or State Terrorism'. If we accept that state actors can perpetrate terrorism, then the recent Stuxnet worm (which is widely regarded as malware of a development standard only made possible through state-sponsorship of some kind (MacLean 2010, Markoff 2011)) does indeed fit the bill of cyberterrorism, as it caused extensive economic damage. However, the very idea of state terrorism is quite controversial (see Primoratz 2005) – as Jeremy Greenstock, the then-Chairman of the UN Security Council Counter-terrorism Committee summarised in the Security Council's 4453rd Meeting, state terrorism is not recognised as a legal concept in the international community: "If States abuse[d] their power, they should be judged against international conventions dealing with war crimes, international human rights and international humanitarian law" ('Addressing Security Council' 2002). The then-Secretary-General of the UN, Kofi Annan, also went on to say that "[e]ach country by itself cannot have its own of special definition of terrorism" ('Press Conference with Kofi Annan' 2002), which specifically problematises the 1975 definitions generated by the USA's Taskforce on Disorders and Terrorism. . In terms of cyberterrorism, we may refer to Vegh (2003) who defines state-associated cyberattacks as 'cyberwar', in keeping with this international legal standard. In summary, as Denning, Arquilla and Ronfeldt's research was both conducted and published prior to '9/11' and seems to endorse this wider understanding of terrorists as non-state actors, their heavy focus on and promotion of the control of the online environment and disapproval of online activism or hacktivism appears to be even more ideologically-based and unjustifiable.

Paul Taylor's (2001) 'Hacktivism: In Search of Lost Ethics' essentially places hacktivism in the slightly updated context of the generations of hacking as formulated by Levy (1984), Jordan & Taylor (1998), Taylor (1999) and Taylor (2000)[14], signifying a second peak in the ethical content of hacking. Apart from recognizing (but not providing empirical evidence) that hacktivism's media image is going the way of hacking's, Taylor contributes little fresh information; the main content of the text is to use Denning's internal framework for hacktivism to explore her examples and a few of his own choosing in a more definitively positive light. Overall, it is somewhat repetitive and disappointing when compared to Taylor's other work on the subject.

4.3.2 Hacktivism and publicity: An unavoidably necessary evil

The final apparently pre- 9/11 text on hacktivism came once more from CAE. *Digital Resistance: Explorations in Tactical Media* (2001) is essentially a critique of the way in which their vision has been operationalised. They reassert their belief that ECD should be a covert tactic in line with the hacker tradition. Courting publicity is "only modestly effective if not counterproductive" (CAE 2001: 11), with activists having no hope of outdoing the massive resources and publicity machines of "capitalist structures" and the media allegiance to the status quo (ibid.: 17). CAE accept that ECD has already been "sold for its 15 minutes of fame", but urge activists to make a concerted effort to engage in actions that provide only "bad copy', thus halting the media event. However, they also argue that ECD must be rescued from the current situation, in which cyberspace trespass or blockage in the U.S. results in jail for a first conviction as opposed to physical CD, which, if actually culminating in an arrest, is punished by a $25 fine and a night's detainment with other protesters.

[14] This has already been discussed thoroughly in the preceding section, but as a reminder: (1) True/Original; (2) Hardware; (3) Software/Game; (4) Hacker/Crackers; (5) Microserfs; and (6) Hacktivism.

> The state can be generous here, since such tactics are purely symbolic in the age of nomadic capital. Such generosity is not shown when the political action could actually accomplish something. This is a situation that must be changed… If we lose the right to protest in cyberspace in the era of information capital, we have lost the greater part of our individual sovereignty. We must demand more than the right to speak; we must demand the right to *act* in the "wired world" on behalf of our own consciences and out of goodwill for all.
>
> (CAE 2001: 33-4, 37)

This final point and their assessment of the dangers of submitting one's cause to the distortions of the mass media and associated institutions are entirely valid. However, it seems all too easy for CAE to criticise the actions of others while remaining safe in their citadel of words. Contrary to CAE's beliefs, dallying with the media is a necessary evil, one that hacktivists cannot escape and can only attempt to manage to their own advantage.

4.4 Hacktivism and the post-9/11 world

The media trend towards the increasing conflation of hacking, hacktivism, and cyberterrorism became even more pronounced following the terrorist attacks on the World Trade Centre 'twin towers' and other American targets. Following 9/11, several authors addressed the intensification of this media trend and the limitations it places upon hacktivism.

4.4.1 Hacktivism and the repertoire of electronic contention

Sasha Costanza-Chock's (2001) 'Mapping the Repertoire of Electronic Contention' has the dubious honour of being the first discussion of hacktivism in a post-9/11 context. He refers to it throughout as ECD (noting that it is commonly referred to as hacktivism elsewhere) but includes tactics such as site defacements and DDoS attacks that have been argued as a poor fit to the term. Borrowing Tilly's (1983) phrase, he proposes a tactic/outcome matrix intended to map out the 'repertoire of electronic contention'. The tactic styles are borrowed from Tarrow (1998), and the outcomes from Staggenborg (1995). The matrix is summarised in Table 6, with the shaded cells identifying those tactics considered to be ECD (Costanza-Chock 2001).

	POLITICAL OUTCOMES	**MOBILISATION OUTCOMES**	**CULTURAL OUTCOMES**
CONVENTIONAL TACTICS	e-lobbying e-petitions non-flooding email and fax campaigns	mobilisation coordination	information distribution alternative news, commentary and publishing oppositional e-art e-fundraising and merchandising e-research representation
DISRUPTIVE TACTICS	campaigns utilising all tactics to the right → and conventional tactics	collective email/fax floods virtual sit-ins	site-defacement and redirection data theft and destruction DDoS attacks automated individual email/fax floods viruses, worms and Trojans
VIOLENT TACTICS	?	←cyberterrorism→	?

Table 6: Costanza-Chock's (2001) tactic/outcome matrix for the repertoire of electronic contention

Costanza-Chock's matrix is a useful framework for considering 'electronic contention' as a whole, but as he admits, there is much actual and potential category overlap, and cyberterrorism is classified as too complex to theorise, presumably because it had not (and arguably still has not) occurred. Nonetheless, the matrix serves to further advance the theoretical differentiation of hacktivism from a wider electronic background. His recognition of the post-9/11 legislative and media trend towards the conflation of hacking/hacktivism and cyberterrorism as limiting the political opportunity structure of disruptive electronic contention and limiting the diffusion of its tactics is also well-founded, despite the lack of supporting empirical evidence.

4.4.2 Hacking for democracy: Media representations of online public resistance to elite control

The status of hacking and hacktivism both before and after 9/11 is one of the subjects of Sandor Vegh's (2003) doctoral thesis, *Hacking for Democracy: A Study of the Internet as a Political Force and its Representation in the Mainstream Media.*[15] The wider focus of Vegh's work is the struggle between elite control and public resistance on the Internet. He conceives of a three-actor model, with the government (privileging national security interests) and corporations (privileging corporate interests) generally united against the wider public and their priority on civil liberties. The basic assertion is that the Internet is a potential tool for democratization if it is allowed and shaped to be, but that as everywhere, "certain counterhegemonic or politically empowering activities are appropriated for the goals of the elite with the help of the mass media under their control to serve as pretext for interventions to preserve the status quo" (Vegh 2003: 32). Hacking and hacktivism are included among these activities, as has been alleged in the previous literature.

[15] Vegh published articles stemming from this in both 2002 and 2005. Both merely repeat thesis content, therefore, the thesis will be primarily focused on.

In line with Manion & Goodrum (2000), Vegh sees a purposive governmental and corporate agenda behind the negative media images, intended to legitimize the installation of oppressive legislature controlling wider political opposition, not just computer crime. Vegh makes a good argument in support of this theory, but it is ultimately exceedingly difficult (if not impossible) to prove. However, this seems less a statement about the author's credibility than about his high ambitions, and he makes an extremely valuable empirical contribution to the discourse on hacking and hacktivism in the media.

4.4.2.1 Differentiating hacktivism from cyberwar, and internally differentiating hacktivists

After outlining a successful framework for strategies of control on the Internet, Vegh similarly attempts to categorise online resistance. The resistant activities are categorised as privacy protection, alternative news, online advocacy, hacktivism, and cyberwar. These categories are claimed to be "exclusive and comprehensive" (ibid.: 132), but considering that the development of software intended to protect the privacy of the user is commonly included amongst hacktivist activities, such as Six/Four and CameraShy, they are somewhat flawed. Vegh's assertion that their techniques may blur but their use will not is too brief to overcome this, and subsequent discussion of examples does not adequately clarify the terminological discrepancy.

Hacktivism and cyberwar are grouped together as cyberattacks, which Vegh proposes should be considered in terms of perpetrator identity, target identity, method of occurrence, frequency of occurrence, goal, and damage caused (ibid.: 165-6). Hacktivism is defined as "a politically motivated single incident online action, or a campaign thereof, taken by non-state actors in retaliation to express disapproval or to call attention to an issue advocated by the activists" (ibid.: 167), with two categories stemming from the hacktivists' background; 'wired activists' or

'political hackers'. (This differentiation is given a more through treatment by Taylor (2004) and Jordan & Taylor (2004), as is discussed later). Cyberwar is defined relatively, as hacktivism "elevated to the state level (in agenda or in terms of actors) and [becoming] a sustained engagement between parties connected to an ongoing conventional armed conflict" (ibid.: 168).

4.4.2.2 Hacktivism and publicity: An unavoidably necessary evil (redux)

Vegh also recognises the reciprocal relationship between the media and hacktivism, likening hacktivists' attempts to garner positive publicity for their cause to an attempt to hack the very process of reporting (ibid.: 199-200). Again, the conclusion is that this is often unsuccessful. Pre-9/11, hacking and hacktivism were feared because of their threat to the networks that had become "the life line of developed post-industrial nations" (ibid., p. 209), and post-9/11, because they are increasingly conflated with cyberterrorism. Even though (as he repeatedly points out) cyberterrorism is still hypothetical, Vegh believes that its media prominence is a function of governmental desire to maintain it as a valid threat, **"**under the disguise of which legislation can be passed that increases the power of the government" (ibid.) (and by association, corporations) and restricts civil liberties and individual rights. Legislative examples are the so-called Patriot Act and proposed Cyber Security Enhancement Act.

Vegh establishes through the quantitative and qualitative analysis of articles from five American newspapers[16] mentioning the word 'hack' or some variant in the year encompassing 9/11, that media coverage of hacking is generally negative and became more so in the 6 months after the attack on the World Trade Centre. Overall trends identified were the tendency to use the conditional tense but overshadow this through the use of strongly negative, sensationalistic language; overuse anonymous 'official sources'; and be vague about the place, time and

[16] The New York Times, Wall Street Journal, Washington Post, San Jose Morning News, and USA Today.

nature of the attacks or attackers, but much more precise when referring to the actual and possible targets. The 'standard nightmare scenario' is again apparent, with air traffic control, nuclear power plants and electrical and water infrastructures the 'usual suspects'. The coverage as a whole became more negative post-9/11, despite a decreased actual incidence of reported hacking and hacktivism[17]. Most significantly, 'attackers' were increasingly identified as cyberterrorists rather than criminals, as part of a larger focus on the subject of cyberterrorism (despite its non-occurrence). This empirical analysis is a major contribution to the literature on hacktivism, finally providing some quantitative proof of hacking and hacktivism's fraught relationship with the mass media.

The 'necessary evil' component of hacktivism's representation in the news media was something that all the Kiwicon organisers and attendees spoken to had similar views on, in that media exposure is often an integral part of successful hacktivism, but that hacktivists need to manage this exposure if it is to benefit them. Several stated that they felt the negative media and public perceptions of hacking were a disadvantage to hacktivist methods when compared with traditional activism, with this 'vilification' and the increasing "privitisation and development of undemocratic mechanisims" online (Farrell 2007) lessening the impact of the political message.

> the challgenges faced are intergral to the paradigm. there is an attempt to fight against what is happening to the online world, however it is these changes that are reducing the capability. there is also the vilification- we are scared to exercise any rights online for fear of being discredited or defamed.
>
> (Farrell 2007)

Metlstorm discussed the publicity prank the Kiwicon organizers used to advertise the conference as an example of the perception management required when utilising hacker or hacktivist techniques in aid of causes, be they political or otherwise:

[17] Vegh argues that this was essentially the result of the majority of hackers and activists wanting to give the U.S.A. 'a break' following the events of 9/11.

the “pranks” we pulled to advertise Kiwicon were pretty good examples of low-level hactivism style techniques, but of course without a political motivation. In this case, we were dissatisfied with the lack of attention paid to our media release, and decided that if the media wouldn’t write our story, we’d write it for them. :) We used XSS (cross site scripting) to inject a fake story into several media sites (and continue to maintain the ability to do so!) to attempt to bait other journalists into reporting on their competitors misfortune. It was effective …

[They used XSS to hack the New Zealand Herald website, one of New Zealand’s major newspapers, and the story was covered by their competitor, the Fairfax-owned Stuff.co.nz website which agglomerates New Zealand’s other major newspapers’ content (see Figure 4: The Stuff.co.nz coverage of the Herald.co.nz XSS 'hack'*). Computerworld.co.nz was also hacked.]*

… The coverage we received for the Kiwicon incidents (IDG’s coverage of it’s own hack, Fairfax coverage of the Herald hack) was sensationalist, and would have been wildly inaccurate had we not ensured that we talked to the journalists and spun things “right”. Reporting of technology issues in the mainstream media is always poor, and if you’re trying to use the media, you have to be very proactive in spin control.

(Metlstorm 2007a)

Figure 4: The Stuff.co.nz coverage of the Herald.co.nz XSS 'hack'

Figure 3 shows the coverage given to the prank by Stuff.co.nz, with Metlstorm's comments explaining that the article was clearly marked as a joke, in that it contained 'wildly unreasonably comment that no sane person would believe" ('Hackers hit NZ Herald website').

4.4.3 Mass Action and Digitally Correct: An internal differentiation of hacktivism

Paul Taylor's (2004) 'Hacktivism: Resistance is Fertile?' generally reiterates previously identified concepts such as hacktivism's relevance in opposing increasingly abstracted capitalist structures and its evolution from the previous generations of hacking. In line with CAE's hopes, Taylor sees hacktivism as a convergence of increasingly politically aware hackers and increasingly technologically 'savvy' activists. However, like Vegh, he argues that these different origins have led to two distinct trends in hacktivism, the first constituted by web hacks and computer break-ins such as site defacements, and the second by acts of ECD such as virtual sit-ins. Little elaboration on these terms is given; hence, it is not precisely clear where their boundaries lie. Hacktivism as a whole is compared to culture jamming, in that it seeks to "reverse engineer global capital" (Taylor 2004: 487); and hacktivists to spiders who spin dynamic webs of resistance on the static networks of global capitalism (ibid.: 494-5). This metaphor is borrowed from Klein (2001) and Lash (2002).

Hacktivism and Cyberwars was also published in 2004, another joint sociological effort from Taylor and Jordan. Like *Hackers: Crime in the Digital Sublime* (1999), it relies heavily on interviews with hacktivists and various statements and manifestos made by different hacktivist groups. As such, it presents a slightly idealised image of the protagonists, though it is a broadly appealing read that offers new insights into potential internal categories of hacktivism. As discussed in the previous section, and as initialized by Taylor (2001, 2004), hacktivism is seen as an ethically resurgent final generation in the evolution of hacking:

> Hackers remain obsessed with a wilful immersion in the abstract environment of computer code, whereas hacktivists connect this immateriality to the importance of a social or political rationale, even when an action is coordinated in cyberspace or is about cyberspace.
>
> (Jordan & Taylor 2004: 35)

The wider context of the information age is the second thread leading into hacktivism, with hacktivism emerging in the lacunae of the "complex communication systems of advanced capitalism… where institutional control becomes increasingly difficult" (ibid.: 20). The mass-mediated vilification of hacktivism is again a function of wider feelings of technological and informational vulnerability. The third thread is simply that of modern social protest and resistance, especially that of the anti-Neoliberal-globalisation movement. Hacktivism is "an attempted solution to the problem of carrying out effective political protest against a system that is expanding its global reach in increasingly immaterial forms" (ibid.: 30).

Hacktivism generally is defined as "a combination of grassroots political protest with computer hacking… Hacktivism is activism gone electric" (ibid.: 1). Expanding on Vegh (2003) and Taylor (2004), two distinct but not mutually exclusive trends are identified within hacktivism. These two categories are dubbed 'Mass Action Hacktivism' (MAH) and 'Digitally Correct Hacktivism' (DCH). MAH is the virtualisation of street protest; effectively ECD, it is "a combination of politics and inefficient technology. It is an attempt to defy the lack of physicality in online life, in favour of a mass collection of virtual bodies that are yet not present to each other" (ibid.: 69). Hacking influences DCH more than street protest; it is "the political application of hacking to the infrastructure of cyberspace. It is an attempt to use the lack of physicality in online life to amplify a political message" (ibid.).

An example of MAH is the use of FloodNet by EDT, which has already been mentioned. Other virtual sit-ins are also included, such as those carried out by the now-defunct Electrohippies as part of the 'Battle in Seattle' in 1999 against the World Trade Organisation (WTO) summit, which reputedly attracted 450,000 participants over five days, and crashed the WTO servers twice (ibid.: 75). Community accountability is privileged; as Ricardo Dominguez said: "All we are

doing is creating the unbearable weight of human beings in a digital way" (Meikle 2002: 142). Parody mirror sites such as those used during the etoy.com/etoys.com conflict[18] and by ®™ark[19] and the 'Yes Men', and other satirical performance-based hacktions are also included under the mantle of MAH.

DCH is generally more interested in the 'bandwidth rights' component of human rights, which can bring some of its proponents and other hackers into opposition with MAH. They see virtual sit-ins as bandwidth abuse, as they can slow down sections of the Internet 'near' but unrelated to their target, which contravenes the hacker ethic privileging the free flow of information. The 1999 use of FloodNet by EDT in support of the Zapatistas actually brought threats from other hackers, who threatened to 'shut them down' in retaliation to their disruption of the network (ibid.: 90). The 'Foreign Minister' of the hacktivist group Cult of the Dead Cow (cDc), Oxblood Ruffin, is cited as calling them "illegal, unethical and uncivil… One does not make a better point in a public forum by shouting down one's opponent" (Ruffin 2002. in ibid.). Others are merely concerned that MAH is inventing "the first self-drowning politics" (ibid.: 167-8).

Hacktivismo, an offshoot of cDc committed to circumventing Internet censorship, have undertaken a number of projects exemplifying DCH, including Peek-a-Booty, Back, Six/Four, and Camera/Shy. These projects will be discussed in more detail later in the thesis, but in short, their intents are as follows. Peek-a-Booty is essentially a distributed anonymous network acting as a server and using cryptographic techniques to elude detection, thus allowing its users or network nodes to bypass firewalls and censorship. For example, a Chinese citizen could use

[18] The etoy.com/etoys.com conflict occurred in 1999 as the result of etoys.com, an online toy store, trying unsuccessfully to buy out etoy.com's domain name. etoy.com are an artist-activist collective, and reacted to the injunction obtained against them by etoys.com by undertaking an online smear campaign, which included parodying the etoys.com site. The result was that etoy.com kept their domain, etoys.com's share price fell 70% over the period of the incident, and they eventually collapsed. Although this could not be linked conclusively to etoy.com's campaign, it seems significant.

[19] ®™ark were a web-based activist group ('RTMark') who essentially attempted to subvert the corporate universe. Perhaps their most infamous stunt was swapping voice boxes of three hundred Barbies™ and G.I.Joes™ then putting them back on the shelves, where they were sold. They created a parody of the WTO website, and a software tool for generating mirror sites for satirical purposes. Their WTO parody site ('World Trade Organisation') was passed over to the Yes Men ('The Yes Men'), two activists who respond to the emails sent to them in error as WTO members, and thus gain the opportunity to give satirical presentations to unsuspecting applicants.

it to safely view a Falun Gong website excluded by the Chinese Internet gateways or servers. Six/Four is similar, while Camera/Shy is a steganography tool that encodes text in images (digital steganography of this kind is the concealment of information within computer files; for example, using the bits or binary code in an image file and modifying them in such a way as to embed a message within the image but have the alterations remain invisible to the naked eye (which is possible due to the huge amount of digital information necessary for image files)). However, there is some concern that DCH may occasionally fall foul of the retrograde hacker tendency to privilege the means of the hack over the end (ibid.: 169).

Jordan's 2008 *Hacking*, although offering new insight into the FLOSS movement, Creative Commons and other 'non-programming' hackers, does not add anything substantial to his and Taylor's previous work. Hacktivism is grouped in with cyberwar, cyberterror, and cybercrime, all of which are collectively described as "hacking the social" (2008: 66). "[T]he social" is defined as "various aspects of the way we live in twenty-first-century societies" (ibid: 70), and is differentiated from 'society' in that these forms of hacking do not address the entirety of what we call society, and simultaneously address extra- or co-societal systems such as politics and economics. These four forms of hacking:

> …address aspects of 'the social' in the following areas: grassroots or popular political activism, conflict between nation states, the nature of security and terror and shifting forms of crime.
>
> (ibid: 70)

The section on hacktivism largely reiterates ideas and cases previously addressed in Jordan and Taylor's previous literature, although what was previously known as digitally correct hacktivism is now described as informational hacktivism. Jordan continues to maintain that mass action and informational hacktivists overwhelmingly gravitate towards different kinds of political issues, a thesis that is borne out within the somewhat dated cases and examples used within the text, but that is arguably increasingly redundant, as is evident in the more recent cases explored within this thesis. Informational hacktivists' focus on the politics of free

informational flows is seen as distinct from those of mass action hacktivists, who apparently "have their eyes firmly on other political issues, particularly those developing from the alter-globalisation movement" (ibid: 76). As Chapter 7 contends, this is an increasingly false or outdated distinction, as there is ample evidence of mass action hacktivism being used to campaign against disruptions to the free flow of information online. Jordan's description of hacktivism as applying primarily to "the politics that dominates the front pages of our newspapers" as opposed to "the politics that dominate discussion in the backroom of IT support" is a clear articulation of this assumed dichotomy (ibid: 71) – technological politics are ever increasingly incorporated into and coterminous with the 'front page' world of mainstream politics, at least within post-industrial societies, and are engaged with by all kinds of hacktivists.

4.4.4 Political coders, performative hacktivists and political cracking: An improved internal differentiation of hacktivism

Furthermore, Jordan & Taylor (2004) and Jordan (2008) fail to discuss web site defacements and other potentially individually undertaken hacktions within their typology. This gap is closed by Alexandra Samuel (2004a) with her doctoral thesis *Hacktivism and the Future of Political Participation.*[20] Samuel uses hacktivism to address three key questions: why do people choose to participate in collective political action; when do political actors pursue policy circumvention rather than policy change; and can the Internet foster new forms of political participation? She defines hacktivism as "the non-violent use of illegal or legally ambiguous digital tools in pursuit of political ends" (Samuel 2004a: iii), differentiated from hacking by its explicitly political nature, from online activism and cyberterrorism in that it is transgressive rather than conventional or violent (see Constanza-Chock 2001), and from traditional CD in that it is online (ibid.: 3-4). Samuel provides a clear and

[20] Like Vegh, Samuel published a book chapter stemming from her thesis (2004). However, only the thesis will be referred to as it encompasses the content of the chapter.

empirically supported internal taxonomy of hacktivism, revealing much about the hacktivists themselves in the process. Furthermore, she begins to place hacktivism within a wider political context, extending upon the intentions of others before her.

	FORMS	ORIGINS	ORIENTATION
POLITICAL CRACKING	Defacements Redirects Automated DDoS attacks Sabotage Information theft	Hacker-programmers	Outlaw
PERFORMATIVE HACKTIVISM	Parodies Sit-Ins	Artist-activists	Transgressive
POLITICAL CODING	Software development	Hacker-programmers	Transgressive

Table 7: Samuel's (2004a) taxonomic matrix of hacktivism

She proposes a taxonomy of hacktivism constructed by the intersection of various hacktivist origins (hacker-programmer or artist-activist) and orientations (transgressive or outlaw). It is built upon and supported by a number of interviews Samuel conducted with hacktivists or those connected to them. Some potential overlap is acknowledged, with the origins recognised as more stable than the orientations (ibid.). Hacktivism that is transgressive in orientation "challenges the legal and political order, but still exists in relation to it and even shares some norms… such as legitimacy and accountability", whereas outlaw orientation "completely rejects the legal and political order" (ibid.: 37). Transgressive hacktivists tend to work in medium-size groups and collaborate multinationally, whereas outlaw hacktivists tend to work solo or in small groups and collaborate nationally, multinationally and internationally. National collaborations target governments, businesses or organisations within their own country; multinational collaborators band across borders to attack a common target at the subnational, national or multinational level; and international collaboration involves hacktivists

from one country targeting a government, business or organisation in another country, sometimes generating reciprocal hacktivism (ibid.: 50). Her taxonomy is best presented in the matrix illustrated in Table 7 (ibid.: 101). It should be noted that performative hacktivism and political coding are analogous to Jordan & Taylor's (2004) MAH and DCH respectively.

4.4.4.1 Hacktivism as a form of identity construction

The question of why hacktivists participate in hacktivism is addressed through the responses given by hacktivists and those associated with them to a questionnaire distributed by Samuel. She argues that hacktivists tend to choose their methods of hacktivism before they choose their political agenda; therefore, Samuel reasons that specific political goals may not always be at the heart of political participation (ibid.: 105-6). She posits that their participation is founded on identity incentives, which "reflect individuals' desire to confirm or enhance their sense of belonging to a group, where membership in that group enhances their self-image or self-esteem" (ibid.: 122). This hypothesis is tested and supported by attempting to predict which form of hacktivism individuals will pursue by their backgrounds. The findings are reflected in the origin component of Samuel's taxonomic matrix.

Furthermore, hacktivists tend to collaborate rather than work alone when there is no real necessity to do so because of instrumental rather than interactive incentives. Hacktivist collaborations are less about social interaction, and more about increased productivity and the desire to affirm one's own identity and self-esteem through affirming that one belongs to a group that shares the same identity and values. Thus, the kind of hacktivism one engages in and the group one collaborates with represent purposive statements about personal identity and values (ibid.: 134).

4.4.4.2 Political coding and policy circumvention

Samuel addresses her second question (asking when political actors pursue policy circumvention rather than policy change) through an assessment of two case studies of political coding, which is almost exclusively concerned with policy circumvention. Policy circumvention is defined as "a strategic political response to a specific policy, law, regulation, or court decision", which aims to nullify the effects of that policy, law, regulation, or court decision. It creates excludable benefits for its individual practitioners, but also some non-excludable benefits such as issue awareness, declining enforceability of the given law, changes in norms concerning policy compliance, and possibly even policy change (ibid.: 156-8). It is important in that it "shunts the state to the status of a side-show whose co-operation is non-essential to obtaining desired political outcomes" (ibid.: 158).

Samuel's case studies support her hypothesis that the emergence and success of any given instance of policy circumvention hinge upon the presence of political entrepreneurs, a low cost of failure ensuring high participation, and a governing state that faces political constraints on repressing the circumvention (ibid.: 164). Policy circumvention is likely to become more common in an increasingly informational society, with increasing political and economic repercussions, and Samuel advises that policies will have to become much more robust and enforceable if they are to hold up to the onslaught (ibid.: 197-98).

4.4.4.3 Hacktivism, free speech, and accountability

Samuel's third question, regarding new forms of political participation on the Internet, addresses hacktivism's challenges to traditional deliberative democratic requirements of free speech and accountability. Hacktions such as site defacements tamper with the speech of others, therefore are they instances of free speech or

actually rebukes to the concept? Performative hacktivists and political crackers work on the belief that access to free speech is not equal, and therefore take an 'ends over means' approach to having their say. This perspective also incorporates the need to have their speech heard, not just spoken, thus, the concept of free speech in the context of the Internet expands to encompass notions of audience access. Conversely, political coders are focused almost exclusively on maintaining an absolute standard of free speech, in line with the original hacker ethic that all information should be free (Levy 1984). This ideological opposition is a reframing of what was discussed in Jordan & Taylor (2004).

Accountability is also problematised by the different nymity practices of hacktivists. Anonymity has been variously theorised as having the potential to be good for deliberative discourse, as it can promote the free flow of ideas, protect unpopular idea from prosecution and privilege the speech act itself rather than the speaker. However, on the down side, it may have a deleterious effect in that it removes accountability, makes it impossible to judge the motivations of the speaker and may even promote uncivil behaviour. Anonymous hacktivism could thus be judged from either perspective. However, through the interviews conducted, Samuel establishes that hacktivists make nymity choices not as a matter of principle but as deliberative statements in themselves, which have the added bonus of further reinforcing their individual and group identity. Political crackers use robust pseudonymity both to avoid legal consequences and declare that they are accountable to no one; political coders use weak pseudonymity to construct a digital persona that is accountable to wider Internet community, but in digital rather than physical terms, and performative hacktivists do not use pseudonyms, thus embracing their accountability to the real world (ibid.: 220). Hacktivists therefore treat their nymity choices as "a political tool, with [different choices] conveying different kinds of claims about political strategy, risk, and above all, accountability" (ibid.; 222).

4.4.5 The imagined community of hacktivism

The identity issues raised by Samuel (2004a) were added to by Still (2005) in 'Hacking for a Cause'. Various reassertions of previously made statements about the evolution of hacktivism and its mass-mediated image issues are made, with Still noting that hacktivists make concerted efforts at clear self-definition and explanation of their motives, not only through the messages contained in their hacktions but by their self-organisation into groups with declarations and codes of ethics (Still 2005). He posits that "the action on behalf of the cause is just as important as the result, especially if that action draws attention to the cause represented by the "hack" and, as a corollary, presents the hacker in a more pro-active, cause-oriented light" (ibid.).

These explicit efforts towards community bounding are in line with Jordan & Taylor (1998), Taylor (1999) and Samuel (2004b). Hacktivist communities are likened to the 'imagined communities' of Benedict Anderson (1983) with their distant but virtually co-present members, and the 'virtual neighbourhoods' described in Appadurai (1996). These neighbourhoods are both created by and creative of hacktivists, as well as being both a product of and having an effect on their wider social environment. Appadurai's observation that they are "often explicitly constituted to monitor the activities of the nation state" (1996: 168, in ibid.) is particularly relevant in light of the criminalisation and conflation with cyberterrorism that hacktivism experiences. This process is again seen as a way for the state to create a 'discourse of danger' (Campbell 1992: 54, in ibid.), and thus normalise truths about how we should and should not behave. Still's article may be little more than a reassertion of the content of previous literature, but these reassertions serve to emphasise central contentions regarding hacktivism.

4.4.6 The morality (or lack thereof) of hacktivism

The final text on hacktivism to be considered is Himma's (2007) 'Hacking as Politically Motivated Digital Disobedience: Is Hacktivism Morally Justified?'. Published as part of a book edited by Himma on computer security, it is essentially a rebuttal of the assertion that hacktivism, understood as electronic civil disobedience, is morally justifiable. As previously argued, the assumption that all hacktivism is or intends to be an electronic form of CD is incorrect. However, Himma's argument can be generalised as an assessment of which instances of hacktivism are morally acceptable (in his opinion). He defines hacktivism as "involving unauthorized digital intrusions for the purpose of protesting some injustice or advancing come political agenda" (Himma 2007: 86). This definition is clearly inferior to that determined by Samuel (2004b) and others, as it does not take into account what Samuel referred to as 'political coding'.

Himma's framework for judging the morality of hacktions is also unsound. The framework considers the magnitude and nature of the harm caused; whether or not the hacktivists are prepared to accept responsibility; whether the hacktivists' political agenda is plausible and supported by adequate reasons; and whether the hacktivists are in cognitive possession of an explanation for their support of this political agenda. Himma considers the most morally justifiable attacks to be on public, non-commercial websites, due to a concern for business losses and the free speech of individuals. Certainly, no instance of a hacktion targeting an individual's personal website springs to mind, but Himma's concern for commercial entities seems either naïve or biased. In terms of accepting responsibility, he feels that hacktivists' frequent pseudonymity does not suffice, and that they should be prepared to accept the legal consequences of their actions. The fact that these consequences would frequently be out of all proportion to the crime seems to escape him. Again, he seems more concerned that their anonymity might cause financial hardship for corporations who feel compelled to spend more on computer security (something which they should really be doing in the first place, in case of truly malicious attacks). He also likens hacktivist groups to terrorists in that they both often operate under group names, although contends that this is "merely to illustrate

that there is morally significant difference between claiming responsibility and accepting responsibility" (ibid.: 90).

He effectively judges hacktivism in support of general human rights and aimed at "oppressive non-democratic governments" as acceptable, but that "in support of the "hacker ethic"" as unacceptable, apparently not considering such rights as open access to the Internet, denied to millions of Chinese, North Koreans and Iranians[21] (regimes one feels sure Himma disapproves of) as part of a wider human rights agenda (ibid.: 91-93). His argument is based on privacy and property rights, and a wilfully literal interpretation of Levy's original three ethics as well as an idealisation of Western democracies as entirely free from human rights manipulations. Lastly, Himma interprets most hacktivism as lacking any clear articulation of their agenda. However, his only example to back this up is site defacements, which are sometimes characterised by unsophisticated political slogans. He does not recognise the overwhelming evidence against his assumption, such as the websites and other documents of many hacktivist groups, which provide pages of motivations and explanations.

Overall, Himma's position seems to be that most hacktivism is morally reprehensible. He sums up by blaming any negative media images of hacktivists on the hacktivists themselves, due to having "committed acts that are far more obviously problematic from a moral view than the positions they seek to attack" (ibid.: 94). This is an almost unbelievably simplistic perspective on the situation, and fails to take into account any wider power structures and political or corporate agendas. Himma's final recommendation is that anonymous hacktivism should be "punished to the full extent under the law" (ibid.: 95), as this will discourage anonymous hacktivism, and deter all anonymous cyberattacks, including, one presumes, cyberterrorism. One would have thought that individuals who are willing to sacrifice their lives for their organisations' cause are unlikely to be dissuaded from cyberterrorism by the prospect of having 'the book thrown at them'. It would seem that all the heeding of this advice is likely to accomplish is numerous hacktivists being punished unnecessarily harshly, effecting a general chilling of moderate and non-violent online political dissent – a trend already encouraged.

[21] Amongst many others.

4.4.7 Hacking and hacktivism: Conclusions and the lack of a public sphere theoretical interpretation of hacktivism

In summary, there has clearly been a reasonable amount of academic attention paid to the subjects of hacking and hacktivism. This is unsurprising; in a rapidly changing and increasingly complex socio-technological environment, it is only natural for the actions of those who are at the forefront of and comfortable with this environmental evolution to be objects of fascination. Understandably, this fascination has been and is shared by the general population, and is coupled with a widespread inability to grasp the full technological complexities of hacking. This is not intended as a condemnation – the average citizen[22] can no more be expected to understand the full technological complexity of computers and the Internet than they can be expected to grasp, say, quantum physics.

However, the difference is that we do not interact with the equipment used by quantum physicists in our daily lives, whereas most of us within the post-industrial world do interact with computers and the Internet on an exceedingly regular basis. At the very least, we understand that they provide a large proportion of our global communications and financial infrastructure, and thus have an immense role to play in facilitating slows of political-economic power. It is this combination of interactional familiarity, reliance, and incomprehension, coupled with an increasing tendency towards malicious activity within certain branches of hacking, that has contributed to the installation of the negative popular image of hacking that exists within society and the mainstream media today. The negativity of this perception is both echoed and reified by ever-increasing and unnecessarily harsh legislative criminalisation of the activity, invoked by state and corporate concerns over its anti-authoritarian nature and tendency towards agendas incompatible with the commercialisation and control of digital information.

This popular perception of hacking has been given much attention within the literature discussed, with a variety of qualitative and quantitative research on the

[22] The author wishes to make it clear that she includes herself in this category.

media's role in promulgating it provided in support. It is also clear that hacktivism if sometimes tarred with the same brush, and that this negative characterisation of both hacking and hacktivism has only been exacerbated since the events of September 11, 2001. Formerly, hacking (and by extension hacktivism) was portrayed and regarded as the online equivalent of offline crimes such as breaking and entering, trespass, fraud and vandalism. As discussed, the sentences applied to such crimes certainly tended to be harsher than those applied to their offline equivalents, arguably due primarily to a legislative fear of the unknown and the desire to discourage a form of crime that is notoriously difficult to detect and control. Nevertheless, the crimes of which hackers stood accused were fundamentally mundane, their glamour imparted largely by their online status and technological sophistication.

However, since the attacks on the World Trade Centre, the demonisation of hacking (and therefore hacktivism, as a branch of hacking) has become more pronounced, as Costanza-Chock (2001) and Vegh (2002, 2003, 2005) have shown. Illegal or borderline-legal hacking of any kind has been increasingly and erroneously conflated with cyberterrorism, just as terrorism has been conflated with Islam. It does not take too much effort to identify the common denominators within these chains of association – a fear of the unknown (be that unknown technological, cultural, political, or religious), and of the fact that everyday technical infrastructures can be subverted and turned back upon those supposedly in control of them. Indeed, is not the hijacking and utilisation of American aeroplanes as weapons against American lives and property nothing if not a massively simple and violent hack, in the original and ephemeral sense of the word?

This conflation attempts to characterise all hacking activity as running counter to democracy and freedom, when the reality is infinitely more complex and nuanced. Certainly, some strands of hacking are criminal and malicious and could never, by any stretch of the imagination, be aligned with democratic values. However, hacktivism is a new form of political participation, as has been explored by some of the literature reviewed. This literature has broadly explored hacktivism's role in democracy, and has begun to explore its function as a form of deliberative

democratic participation, and as such, has briefly engaged with public sphere theory.

However, this theory has been paid only minimal attention within the literature, and what attention it has received has been rather shallow and unsatisfying. It has largely been passed over in favour of investigations into the sociology of hacking and hacktivism; into categorically defining hacktivism's emergence from the evolutionary tree of hacking; into the construction of typologies to demarcate different groups and group identities within hacktivism; and into the crisis of public perception suffered by all hacking, be it political or not. This is not to say that these projects are invaluable – far from it. They have served to lay down a foundation that facilitates and eases the continued and extended study of the subject area. Indeed, the concentrated application of public sphere theory to the phenomenon of hacktivism is a logical investigative path revealed by some of this prior literature. Vegh (2003) and Samuel (2004a) in particular have tangentially highlighted its appropriateness to the study of hacktivism, and as such, have substantiated the presence of a direction for new research.

Vegh (2002, 2003, 2005) assessed hacking and hacktivism from a broad democratic theory perspective, using it as a window with which to explore his thesis that the U.S. government and corporations use the media to negatively characterise politically empowering Internet-based activities, in order to legitimise the installation of oppressive legislature and thus control widespread instances of political opposition. However, his engagement with both online and offline democracy theory is somewhat scattered and unfocused – he does not engage strongly with any one particular theory. His interest lies more with the general democratising potential of the Internet and the forces opposing it, than with assessing this potential through any strongly coherent and well-defined theoretical lens.

This is even truer with regards to his discussion of hacktivism – it is regarded as a form of democratic political participation *per se*, rather than this status being explored through any particular theoretical lens. This is not to say that this assumption is wrong, just that it is worthy of deeper and more complex attention and investigation. A more thorough exploration of *how* exactly hacktivism

functions as form of democratic political participation is required. Additionally, while Vegh does refer to the concept of the public sphere several times in passing, he does not rigorously examine or apply it with any theoretical complexity, depth, or precision, and certainly not with regards to hacktivism, merely with regards to the Internet in general.

Samuel (2004, 2004a) engages with the concept of deliberative democracy a little more deeply, but it is essentially tangential to her primary goals of investigating the motivations for and forms of political participation, and the relationship of these to the identity of participants. Her assessment of hacktivism's relation to the traditional deliberative values of free speech and accountability is perceptive and valuable, but like Vegh, the democratic theory she deploys is quite broad, and does not home in on any strongly unified theoretical subsection, or engage significantly with (any particular) concept of the public sphere. It should be noted that these comments regarding Vegh and Samuel's work are not intended as criticisms – both authors have made intensely valuable contributions to the literature on hacktivism within their own particular theoretical fields and approaches. But they are the two contributors to the literature on hacktivism who have come closest to assessing it through the lens of public sphere theory, and neither has done so adequately (an understandable omission, given that this was not the intent of their theses).

Following from this deficiency in the literature on hacktivism, this thesis will explore hacktivism through a public sphere theoretical lens. Before proceeding to the theoretical chapters that focus this lens, let us first briefly recap the definitions of hacking and hacktivism that have emerged from the literature review as a whole.

4.5 A summary of the literature and emergent definitions

4.5.1 A 'definition' of hacking

As the last two chapters have shown, there is little doubt that hacking is "one of the buzzwords of the computer age" (Vegh 2003: 151). Yet the definition of the action, and of its actor, the hacker, remains mercurial. As we have seen, the origin of the terms and the identity they refer to is obscure, and they have been and are used in a variety of contexts and connotations.

Despite this ongoing disagreement over even its most basic level of meaning, hacking is arguably best understood as a playful, creative, ingenious interaction, modification or manipulation of an object or subject, often in a manner originally unintended for that object or subject. A certain spirit inherent in the activity remains constant, but the actor, their intent, and that which is acted upon do not. Fashion, craft, architecture – any aspect of life can, theoretically, be hacked. People or 'wetware' can be hacked. Hardware can be hacked. And, of course, computer systems and networks can also be hacked.

These latter types of 'hackable objects' (computer systems and networks) support the most common general meaning of 'hacking', but even this narrowed categorisation contains fractures and contradictions. As the seven generations previously identified attest, 'computer hacking' has been and is used to mean rather different things. Are hackers 'heroes of the computer revolution' (Levy, 1984), or are they 'electronic bogeymen'? Do they hack for fun, 'kudos', political reasons, or out of greed and malignancy? Is what they do illegal, or does it represent a particular work ethic and means of production? The answer is all of the above, and more. Computer hacking has been occurring for six decades, and the practice has evolved in numerous directions, for numerous reasons, and with numerous outcomes. It is highly heterogeneous and polysemic.

This floating polysemy has left the terms hacking and hacker vulnerable to attempts at external meaning making and fixing. Governments and corporate media often frame hackers as purely criminals or terrorists, conflating the term with the practices of cracking for personal gain our out of malice, or with cyberterrorism or cyberwarfare. These practices are certainly branches on the evolutionary tree of computer hacking, but they are not particularly representative of the practice at large. The programmers 'hacking up' code for money or love, for proprietary or free/open source projects, at work, at home, and in hackspaces, not to mention 'ethical hackers' or computer security professionals, are all hackers. They quite possibly comprise the vast bulk of the global hacker community in terms of sheer numbers. They are simply not as 'newsworthy' as those hacking into a power plant's SCADA system or a bank's credit card records, or into Google, Adobe or Intel's corporate network.

Hacking should be understood as a practice, approach or toolkit. What it is ultimately used *for* can vary widely. It is a means, not necessarily an end in and of itself (although many hackers do see hacking as inherently enjoyable).

4.5.2 A comparative definition of hacktivism

Hacktivism, broadly defined, is an amalgamation of the techniques and ideologies of traditional activism or protest with the techniques and ideologies of hacking, in the aid of a political cause or ideology. Given the floating polysemy of the term 'hacking', this is not a particularly precise definition. However, we can at least narrow down the hacking component of hacktivism to that associated with and done on computers and computer networks, and particularly on the Internet. This still leaves us with a multitude of possible hacktivist activities, but this diversity of form is one of the fundamental characteristics of hacktivism – it is not so much what is done (as long as it causes disruption as opposed to damage, as will be summarised shortly), but who it is done by and why it is done that defines an activity as hacktivism or not. The New Zealand hackers spoken to agree with this intent- as

opposed to action-based definition. When presented with a list of possible forms of hacktivism (such as virtual sit ins, defacements, software production, etc), all concurred that any form of activity interpretable as computer hacking can be defined as hacktivism, if it is designed and enacted in aid of a political cause.

> Basically any of the activities could be if the motivation is to promote a particular ideology. Likewise none would be if ideology promotion is not the motivation, each act would need to be judged on its own merits.
>
> (Parsons 2007)

We can further narrow down our definition of hacktivism if we understand it not only for what it is, but also for what it is not. It shares the broader definition of 'hacking for a political cause' with both cyberterrorism and cyberwarfare, but is differentiated from these practices through their perpetrators and their effects. As such, synthesising from the literature reviewed, we may expand our previous definition as follows.

Hacktivism is an amalgamation of the techniques and ideologies of traditional activism or protest with the techniques and ideologies of hacking, in the aid of a political cause or ideology. Hacktivism is demonstrably politically motivated, and is disruptive without resulting in human, infrastructural or serious financial casualties. It may be peripherally aligned with an ongoing conventional armed conflict, but its perpetrators have no direct governmental, military or diplomatic connections. Any form of activity interpretable as hacking (with hacking being understood as a creative, ingenious interaction, modification or manipulation of an object or subject, often in a manner originally unintended for that object or subject) that is associated with and done on or with computers and computer networks, and particularly on the Internet, can be used in hacktivism.

In contrast, cyberwarfare is politically motivated hacking of any kind that is directly connected to ongoing conventional armed conflicts, and is perpetrated by the governments and militaries involved in them. It may be merely disruptive, or it may

result in human, infrastructural or serious financial casualties. An example is the 2008 crippling of the Georgian communication system, timed to coincide with the Russian military strike and apparently committed by government-directed hackers, as revealed in the 'Grey Goose' reports ('Grey Goose 2' 2009). Finally, the definition and indeed existence of cyberterrorism is somewhat contested ('Cyberterrorism' 2009), but it is essentially "the convergence of cyberspace and terrorism. It covers politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage" (Denning 2001: 241), perpetrated by terrorists, understood in the broad sense of being violent non-state actors (Mendelsohn 2005).

4.5.3 An internal typology of hacktivism

Hacktivism also has an internal typology, as the convergence of increasingly politically aware hackers and increasingly technologically savvy activists has led to several distinct trends within the practice.

Jordan and Taylor first proposed a typology to make sense of these trends, identifying 'mass action' (MAH) and 'digitally correct' (DCH) hacktivism as two distinct sub-forms of hacktivism (2004). MAH draws upon street protest and civil disobedience, thus connecting most strongly with the activist origins of hacktivism. It *defies* "the lack of physicality in online life, in favour of a mass collection of virtual bodies that are not yet present to one another" (ibid.: 69). Virtual sit-ins and satirical performance-based hacktions such as the parody mirror sites of ®™ark and the Yes Men, are MAH. DCH, in contrast, *use* "the lack of physicality in online life to amplify a political message" (ibid.: 6). True to its hacker roots, DCH is often in aid of 'bandwidth rights', which sometimes brings it into conflict with MAH. The group 'Hacktivismo', with its overarching aim of circumventing Internet censorship, exemplifies DCH.

However, Jordan and Taylor's proposed typology, while accurate and useful, is incomplete. It does not account for website defacements and other potentially individually undertaken hacktions. Samuel (2004a) closes this taxonomic gap, providing us with an empirically grounded matrix of hacktivist origins (hacker-programmer or artist-activist) and orientations (transgressive – challenging the legal and political order but still existing in relation to it, or outlaw – completely rejecting the legal and political order) (2004a: 37). 'Performative hacktivism' is done largely by artist-activists, and takes transgressive forms such as site parodies and virtual sit-ins. Jordan and Taylor's concept of MAH can be seen as the rough forerunner of this category. 'Political coding' is done largely by hacker-programmers involved in transgressive software development, and succeeds Jordan and Taylor's concept of DCH. Her additional category, 'political cracking', is usually carried out by hacker-programmers, and consists of outlaw permutations such as DDoS attacks, information theft, the use of viruses/trojans, and site alterations/redirections. Although the usage of the term 'cracking' is arguably inappropriate, the categories themselves provide a sophisticated typology. They are not rigid – the potential for overlap is recognised (2004a: 3-4) – but they provide an invaluable interpretive guide (see Table 8).

ORIENTATION/ORIGIN	HACKER-PROGRAMMER ORIGIN	ARTIST-ACTIVIST ORIGIN
TRANSGRESSIVE ORIENTATION	Political Coding (DCH)	Performative Hacktivism (MAH)
OUTLAW ORIENTATION	Political Cracking	-

Table 8: Samuel's (2004a) typology of hacktivism, with Jordan & Taylor's (2004) categories inserted.

Having armed ourselves with these definitions and typologies, we must complete our scholarly arsenal with strong understanding of public sphere theory. This body of theory is not unified but fragmented, so we must also define which particular conception of the public sphere is to be used. The following chapters take Habermas's original conception of the public sphere as their starting point, and through a thorough assessment of the various critiques and reformulations associated with this original concept, synthesise a new understanding of the public sphere. This 'neo-Habermasian public sphere' is based upon the 'radical' or 'agonistic' tradition, and provides a more thorough comprehension of issues of power and difference.

Chapter 5

The Habermasian public sphere

The popularity and significance of deliberative democracy theory has risen in response to increasing dissatisfactions and disillusionment with the theories and realities of aggregative democracy. Deliberative democracy aims towards transcending the crude aggregation of egotistical individual preferences by fostering the engagement of citizens in free, rational deliberation and debate, in which individual preferences are tested against others', and are thus improved upon – the force of the better argument prevails, and an understanding is reached. "[E]gocentric calculations of success" are shunned (Dahlberg 2005: 111). This unconstrained, rational deliberation takes place within, and simultaneously constitutes, the public sphere (or spheres).

The concept of the public sphere is rather complex and there is much disagreement over its exact meaning (as will be explored fully in this chapter and the next), but its primary value lies in the way that its health constitutes "a concrete manifestation of society's democratic character and thus in a sense the most immediately visible indicator of our admittedly imperfect democracies" (Dahlgren 1991: 2). It provides a category against which the political communication of citizens in contemporary democracies can be assessed, and an ideal model to work towards. "Its purpose is to help identify, critique, and challenge blockages to free and critical communication so that we can *move towards* the idealised public sphere and rational public opinion" (Dahlberg 2005: 127).

In order to usefully investigate hacktivism through the theoretical lens of the public sphere and deliberative democracy, it is necessary to first conduct a thorough investigation of what exactly we believe the public sphere to be. A broad conception of the public sphere has existed since Ancient Grecian times (Habermas 1989: 4; Weintraub & Kumar 1997, in Butsch 2007: 3), and some version of it has always been linked to democracy (Dahlgren 1991: 1), but the theoretical treatment of the concept has progressively evolved into greater complexity, and has also been

multiply extended through the attention of several different schools of thought and contextual perspectives. This extension has stretched the concept in several directions, not all of which are mutually compatible, leaving the theoretical field more networked than linear in character. As such, for the sake of coherency and conviction, it is necessary to confer allegiance on the network subsection seen as the most legitimate. However, the explication of this is best achieved in a radial fashion, starting with the network hub and exploring directionally outward. As such, we must start here, with a through investigation of the core public sphere theory of Jürgen Habermas, the German academic widely regarded as "central to discussions about a public sphere in modern democratic societies" (Edwards 1992: 127).

5.1 *The Structural Transformation of the Public Sphere*

As has already been explained, the textual hub around which the vast majority of contemporary public sphere theory revolves is Jürgen Habermas's *The Structural Transformation of the Public Sphere; An Inquiry into a Category of Bourgeois Society* (which will henceforth be truncated to *Structural Transformation*). First published in 1962 in the author's native German (as *Strukturwandel Der Öffentlichkeit; Untersuchungen Zu Einer Kategorie Der Bürgerlichen Gesellschaft*), it quickly generated much critical attention, which was revived and extended with its English translation in 1989. This attention has shown little sign of flagging in the years since, attesting to the continuing power and relevance of both the concept in general and Habermas's analysis in particular.

5.1.1 Habermas and the Frankfurt School

Habermas is one of the younger (and hence, surviving) members of the 'Frankfurt School' of critical theory, based in the Institute for Social Research (*Institut für Sozialforschung*) at Frankfurt University. He began his studies in philosophy and sociology there in 1956, under the tutelage of Theodor Adorno and Max Horkheimer. *Structural Transformation* was written as a *Habilitationschrift* or post-doctoral dissertation, required for ascendancy to Professorship, but Adorno and Horkheimer rejected it. There is some debate as to why exactly this was; Calhoun claims that it was because they both found it insufficiently critical of liberalism (1992: 4), in contrast to Wiggerhaus, who states that while Adorno found it acceptable, Horkheimer found it too radical, and demanded revisions that Habermas was not prepared to make (1996: 555, in Kellner 2000: 3). It is unclear which account is correct, but the fact that in 1964 Habermas took over Horkheimer's chair in sociology and philosophy at the Frankfurt School, with the strong support of Adorno, seems to give credibility to Wiggerhaus's version. In any event, Habermas successfully submitted *Structural Transformation* to the University of Marburg, and completed his *Habilitation* under Wolfgang Abendroth, publishing *Structural Transformation* as his first book in 1962.

Despite its rejection by Habermas's mentors, *Structural Transformation* is a clear product of the Institute for Social Research, both in its multidisciplinary approach and its criticism of the decline of democracy. It combines elements of sociology, economics, constitutional law, political science, and socio-cultural history; a daunting undertaking which Habermas himself acknowledges is more than any one author has the power to master in full (1989: xvii). However, it is also an attempt to escape from the "pessimistic cul-de-sac" of the Institute (Calhoun 1992: 5), in that it ultimately calls for the renewal of democracy and provides a theory pertinent to this process.

5.1.2 The rise of the bourgeois public sphere

Structural Transformation is primarily a historical and sociological analysis of the rise, transformation, and decline of the historically specific Westphalian-national bourgeois public sphere within England, France, and Germany. The public sphere was simultaneously a category of bourgeois society and constitutive of it: "the reorganisation of society around the institutions of public criticism was one of the means by which bourgeois society came into being, conscious of itself as 'society'" (Warner 2002: 48). Habermas's investigation is of the bourgeois public sphere "created out of the relations between capitalism and the state in the seventeenth and eighteenth centuries" (Calhoun 1992: 5), but his underlying motive is to salvage the public sphere ideal "from its historically contradictory and partial realization" within the actual bourgeois public sphere (ibid.: 4). The public sphere ideal that emerges is a sphere between the private and public realms of life, where private people come together as a public, bracketing their private particularities and statuses in order to engage, as equals, in rational-critical debate over matters of public interest. Its separation from the state allows it to function as a critical check upon and a guide to state activity.

Habermas begins with a discussion of the pre-Enlightenment feudal form of representative publicity, status attributes through which the royalty and aristocracy "represented their lordship not for but 'before' the people" (Habermas 1989: 7). He then traces the emergence of finance and trade capitalism in Europe in the thirteenth century. This was initially incorporated smoothly into status quo power relations, but long distance trade required an ever-more regular and exact trade in information about distant happenings, and the private postal and trade newsletter service that emerged in response to this demand would prove the catalyst for a new social order (ibid.: 15-16). The news contained in these newsletters was soon recognised as a generally saleable commodity, leading to the rise of the public press in the mid-seventeenth century. By the latter third of this century, the public journals and periodicals were providing not only information but also criticism and reviews (ibid.: 25). Initially, this press was "systematically made to serve the interests of the

state administration" (ibid.: 22), with rulers directing the contributions of the emergent bourgeois strata of administrative officials, doctors, church officials, intellectuals, and various capitalists (merchants, bankers, entrepreneurs, and manufacturers) (ibid.: 23). However, this would soon change, and the critical light of the press would soon be turned upon authority, compelling it to "legitimate itself before public opinion" (ibid.: 25-26).

At around the same time, English coffeehouses, French *salons*, and German *Tischegesellschaften* (table societies) and *Sprachgesellschaften* (literary societies) emerged, within which intellectuals, nobility and mercantile bourgeoisie mingled as a public, discussing and criticising literature, art and music (ibid.: 33-43). This artistic debate gradually spread to political-economic debate, and despite differences in size, procedural style, debate climate and main concerns, was characterised in all these public institutions by "a kind of social intercourse that, far from presupposing the equality of status, disregarded status altogether" (ibid.: 36). Furthermore, discussion regularly problematised areas and issues that had not previously been questioned, and participation was, in principle, wholly inclusive: "The issues discussed became 'general' not merely in their significance, but also in their accessibility: everyone had to be *able* to participate" (ibid.: 37).

This habit of literary criticism was part of a wider popularisation of reading amongst the bourgeoisie. This arose, in part, because of a peculiarly bourgeois focus on the private, autonomous sphere of the family, and individual introspection and self-constitution via this familial unit (ibid.: 44-48). This resulted in a widespread "exploration of self-subjectivity" through letter writing (ibid.: 49). These letters were commonly written with the expectation that they might become public, and indeed, those of notable individuals were frequently published. This 'age of letters' led to a popularisation of fiction novels written in a serial or letter form, and a corresponding surge in literary society membership. These societies re-articulated the public that had outgrown the salons and coffeehouses and was holding itself together through the press. The institutions of and skills developed within this rational-critical literary public sphere provided the platform for the ascendance of the political public sphere in the eighteenth century (ibid.: 51-52). The political public sphere opposed itself to absolute sovereignty, and "articulated

the concept of and demand for general and abstract laws and [which] gradually came to assert itself (i.e. public opinion) as the only legitimate source of this law" (ibid.: 53). The public opinion in question was "born of the power of the better argument", rather than through coercion or manipulation (ibid.).

The political public sphere first arose in Britain, in the eighteenth century. It was prefigured by the rise of the press as "a genuinely critical organ of a public engaged in critical political debate: as the fourth estate" (ibid.: 60); the demotion of the king to merely another member of parliament (ibid.: 63); and an increase in the size and frequency of public meetings (ibid.: 65). The same process occurred in France, albeit at a much slower pace, but once the state debt accrued by Louis XVI was made public in 1781, the public sphere in France could no longer be eliminated, only repressed (ibid.: 67-68). Soon after, the French revolution achieved practically overnight (though admittedly, less stably) what had taken Britain the course of a decade. "Club-based parties emerged from which parliamentary factions were recruited; there arose a politically oriented daily press" (ibid.: 70). In 1771, the public sphere gained constitutional protection, and although this was soon quashed by Napoleon, the privileged status of the public sphere was gradually regained over time (ibid.: 71). The public sphere was simultaneously emerging in Germany, but due to the fact that the bourgeoisie kept themselves much more separate from the nobility than in England or France, and the stronger dependence of the nobility on the courts, it was somewhat weaker and more limited than elsewhere. However, the bourgeois strata did manage to participate through reading societies, based around political journals and debate (ibid.: 72-3).

Nonetheless, by the start of the nineteenth century, the public sphere was in existence throughout these three nations, which had gradually transformed into bourgeois constitutional states. The public sphere may be conceived of as above all "the sphere of private people come together as a public" to engage the authorities in a debate over the general rules governing relations in the sphere of commodity exchange and social labour. "The medium of this political confrontation was peculiar and without historical precedent: people's public use of their reason (*öffentliches Rässonenment)"* (ibid.: 27). It was, in principle, open to all, and

participants were expected to 'bracket' their private status in order to deliberate rationally over matters of common or public interest.

The public sphere was constitutionally protected through the upholding of rights such as free speech, freedom of assembly, equality under the law, and so on. Its establishment corresponded with a move towards free market trade and *laissez faire* economics, and a faith that these logics would "function in a fashion that ensure everyone's welfare and justice in accord with the standard of the individual's capacity to perform" (ibid.: 79), hence ensuring a society free from coercion and domination. State laws were expected to be similarly impartial; however, unlike market function, these needed to be "explicitly enacted" (ibid.: 80). The public sphere was the method through which legislative guidance was effected. "The constitutional state as a bourgeois state established the public sphere in the political realm as an organ of the state so as to ensure institutionally the connection between law and public opinion" (ibid.: 81). The public debate enacted within the public sphere "was supposed to transform *voluntas* into a *ratio* that in the public competition of private arguments came into being as the consensus about what was practically necessary in the interest of all" (ibid.: 83). All parties affected by the deliberation were, in principle, included, and rational-critical debate and consensus on the common or public good was secured through the bracketing of status and transcendence of private interests within deliberation.

5.1.3 The rationalisation of exclusion

However, in stark contrast to this egalitarian rhetoric, there were still massive power inequalities within society. Despite the public sphere being prefigured on an ideal of perfect inclusiveness, many citizens (predominantly the proletariat) were excluded from participating in it. The public sphere was almost exclusively the domain of educated property owners. Given that it was recognised that "[a] public sphere from which specific groups would be *eo ipso* excluded was less than merely incomplete; it was not a public sphere at all" (ibid.: 85), this seems highly

problematic. However, a peculiar logic based on the belief in the equalising power of the free market allowed this seemingly blatant contradiction to be rationalised out of existence.

Exclusion from the public sphere was seen as acceptable if it could be viewed as simply the "legal ratification of a status attained economically in the private sphere, which is to say, the status of the private person who was both educated and owned property" (ibid.: 85). The belief that the socio-economic conditions gave "everyone an equal chance to meet the criteria for admission: specifically, to earn the qualifications for private autonomy that made for the educated and property owning person" (ibid.: 86) legitimised wide-ranging and systematic exclusions from the public sphere. Thus property owners or *bourgeois* became coextensive with *homme*, or human beings as such. These two roles were combined under the common title of the 'private', and this was the space from which the political self-understanding of the bourgeois public stemmed (ibid.: 29). Clearly, as has since been repeatedly illustrated, the proclamation that a free market will realise a great leveling of society by providing the means for upward socio-economic mobility is not only false, but also ideological. It obscures a continual reification of status quo power relations. Then, as now, those who owned property (of any sort) were primarily those who gained education, and those who gained education were the ones who achieved property ownership. It was, and is, nigh on impossible for the vast majority of society to break into this cycle, hence, a continual re-entrenchment of dominance occurs.

And indeed, this was exactly the case with the bourgeois public sphere. The identification of "property owner" with "human being as such", or legitimate participant within the political public sphere, generated a public sphere within which "the interest of class, via critical public debate, could assume the appearance of the general interest, that is, in the identification of domination with its dissolution into pure reason" (ibid.: 88). Habermas's engagement with the work of Karl Marx within *Structural Transformation* illustrates in detail this internal contradiction of the public sphere. Marx saw public opinion (as generated within the bourgeois public sphere) as a false consciousness that concealed class interests, and in its

opposition to proletarian interests, is fundamentally demoted to the status of a particular rather than public interest (ibid.: 125).

> [T]he dissolution of political domination in the medium of the public engaged in rational-critical debate did not amount to the purported dissolution of political domination in general but only to its perpetuation in different guise. The bourgeois constitutional state, along with the public sphere as its central principle of organisation, was mere ideology. The separation of the private from the public realm obstructed at this stage of capitalism what the idea of the bourgeois public promised.
>
> (Habermas 1989: 125)

However, Marx's belief that the extension of the public sphere within a class society was impossible, and that a revolution was imminent, was incorrect. The proliferation of the press and propaganda in the nineteenth century catalysed the informal extension of the public sphere. With the beginnings of this expansion in participation, the internal contradiction stabilised by the specific context of the bourgeois public sphere was brought to the fore (ibid.: 88), undermining the coherence afforded by institutions of sociability and a relatively high level of education (ibid.: 132). The needs of the proletariat, clearly unable to be satisfied by a self-regulating market, demanded fulfillment via state intervention. The public sphere, which now had to deal with these demands, became an arena of competing interests fought out in increasingly non-rational-critical ways.

5.1.4 The fall of the bourgeois public sphere

The liberalism of Mill and Tocqueville illustrates vividly the crisis experienced within the public sphere due to the exposure of the internal contradiction it harboured. While recognising that a belief that the latent equality in the private economic sphere also maintained open access to the public sphere was no longer

credible, and favouring, in principle, the opening up of the public sphere to the uneducated, unpropertied classes, they did not favour the effect this process had:

> …the unreconciled interests which, with the broadening of the public, flooded the public sphere were represented in a divided public opinion and turned public opinion… into a coercive force, where it had once been supposed to dissolve any kind of coercion into the compulsion of reason.
>
> (Habermas 1989: 133)

They saw public opinion as degenerating into "the reign of the many and the mediocre… more of a compulsion towards conformity than [as] a critical force" (ibid.: 133), in line with Mill's thesis of the 'tyranny of the majority'. The political public sphere was no longer functioning with the intention to *dispel* power; instead, it was merely generating public opinion aimed at *limiting* power:

> …the contours of the bourgeois public sphere eroded… While it penetrated more spheres of society, it simultaneously lost its political function, namely; that of subjecting the affairs that it had made public to the control of a critical public.
>
> (Habermas 1989:140)

5.1.4.1 The refeudalisation of society and the public sphere

Society, and the public sphere, underwent what Habermas calls 'refeudalisation' on a grand scale. "[U]nder conditions of imperfect competition and dependant prices social power became concentrated in private hands" (ibid.: 144), and with the extension of participation in the public sphere, it became an increasingly unfit

platform for the resolution of conflicts within society. Weaker economic actors appealed to the state for help, generating a conflict of organised interests, all trying to influence legislation in their favour. This resulted in increasing state interventionism, which structurally transformed the relationship between the private and public spheres that served as the base for the bourgeois public sphere. The masses had succeeded in transforming economic antagonisms into political conflicts, hence establishing a continuing connection between the asymmetric accumulation of capital and increased state interventionism. In general, state interventions "were guided by the interest of maintaining the equilibrium of the system which could no longer be secured by way of the free market" (ibid.: 146).

State interventionism took the form of not only the expansion of traditional functions, but the assumption of new ones as well. The state had already been involved with protecting, compensating, and subsidising weaker segments of society, but began attempting to actively shape long-term changes in the social structure. It simultaneously took over services previously left to the private realm, by assigning private entities to public tasks, coordinating and planning private activity, and becoming actively involved in production and distribution (ibid.: 147). The social welfare state was born.

With this, the previously private realm of the family became public. A reliance on the state robbed families of their autonomy, and they increasingly lost control over their own education, protection, care and guidance. Individual family members were now being socialised more by society directly, rather than within the familial unit. However, a simultaneous gain in consumption ability and function gave the illusion of an intensified privacy, generating a pseudo-private state of being. Through consumption-based leisure activities, citizens increasingly came under the influence of semi-public authorities. In general, there was a paradigm shift from a culture-debating to a culture-consuming public (ibid.: 155-160). The private sphere became pseudo-public, and the public sphere, pseudo-private. This interpenetration between spheres, the 'societalisation' of the state and 'stateification' of society destroyed the constitutive basis of the bourgeois public sphere.

5.1.4.2 The role of the mass media

> When the laws of the market governing the sphere of commodity exchange and social labour also pervaded the sphere reserved for private people as a public, rational-critical debate had a tendency to be replaced by consumption and the web of public communication unravelled into acts of individuated reception, however uniform in mode.
>
> (Habermas 1989: 161)

This hollowing out of the public sphere was facilitated in large part by the mass media. Mass-mediated leisure activities, taking place within a social climate and privileging a private form of appropriation, "removed the ground for a communication about what had been appropriated" (ibid.: 163). Certainly, debate still regularly occurred and occurs, but it had and has been commercialised. We, for the most part, purchase the watching of or listening to debates, rather than participating ourselves.

> Discussion, now a "business", becomes formalised; the presentation of positions and counterpositions is bound to certain prearranged rules of the game; consensus about subject matter is made largely superfluous by that concerning form.
>
> (Habermas 1989: 164)

Literature has been 'dumbed down' and made cheaper, so more are able to access it, and the new electronic media (radio and television, at the time of Habermas's writing) eradicate the rational-critical form of communication privileged by serious reading. They foster no critical debate, only discussion about consumer preferences (ibid.: 171). While "serious involvement with culture produces facility… the consumption of mass culture leaves no lasting trace; it affords a kind of experience which is not cumulative but regressive" (ibid.: 166).

Furthermore, the mass mediation of the public sphere results in the assumption of advertising functions, hence it becomes "deployed as a vehicle for political and economic propaganda", contributing to its further de-politicisation and pseudo-privatisation (ibid.: 175). The commercialisation of the press and media renders them manipulable; they become the "gate through which privileged private interests [invade] the public sphere" (ibid.: 185), and instead of merely transmitting or amplifying debate, the media have come to shape the debate (ibid.: 188). The critical publicity of the public sphere has transformed into manipulative publicity, with the publicity displayed by elite private interest groups (who are among the few who can afford to participate in the commercially mediated public sphere) via publicity work or public relations, reminiscent of the performative or representative publicity displayed by feudal kings.

Additionally, "because private enterprises invoke in their customers the idea that in their consumption decisions they act in their capacity as citizens, the state has to "address" its citizens like consumers. As a result, public authority too competes for publicity" (ibid.: 195). Hence, the public sphere is comprehensively refeudalised, and publicity is generated from above, in order to secure the agreement or acquiescence of the masses, but not to engage them in debate (ibid.: 177). Societal domination is exercised through the "domination of non-public opinion: it serves the manipulation *of* the public, as much as legitimation *before* it" (ibid.: 178) - "[t]he public sphere becomes the court *before* which public prestige can be displayed, rather than *in* which public critical debate is carried out" (ibid.: 201).

The political process becomes a hollow shell of its former self, lacking in dynamism and legitimacy. Political debate amongst citizens is rarely critical, and often takes place only within close social groups, who are frequently politically homogenous to begin with. Superficial, personality-based electioneering eclipses substantive issues, and mediated political publicity is usually oriented towards swing-voters, who tend to be relatively uninformed and acknowledgeable. As such, this publicity is geared towards shallow manipulation rather than information. The main body of voters are dogmatically party allegiant, influenced by opinion-leaders in society and are hence barely worth appealing to (ibid.: 213-215). As a result, voting (the main means by which citizens are given democratic political expression in modern

representative democracies) is overwhelmingly illegitimate, because the political opinions informing it are not formed rationally, nor are they formed via deliberation or discussion.

3.1.4.3 The modern 'public sphere' and the possibility of renewal

> Thus a public of citizens that had disintegrated as a public was reduced by publicist means to such a position that it could be claimed for the legitimation of political compromises without participating in effective decisions or being in the least capable of such participation.
>
> (Habermas 1989: 216)

Due to the transformation of the public sphere, "[t]he process of the politically relevant exercise and equilibration of power now takes place directly between the private bureaucracies, special-interest associations, parties, and public administration The public as such is included only sporadically in this circuit of power, and even then it is brought in only to contribute its acclamation" (ibid.: 176). Hence, the world and political system endorsed and "fashioned by the mass media is a public sphere in appearance only" (ibid.: 171). Overall, Habermas believes that "the occupation of the political public sphere by the unpropertied masses led to an interlocking of state and society which removed from the public sphere its former basis without supplying a new one" (ibid.: 177). He concludes by offering tentative proposals for the revitalisation of the public sphere, by "setting in motion a critical process of public communication through the very organizations that mediatise it" (Habermas 1989: 232), although he fails to provide any strategies or concrete proposals for this (Kellner 2000: 6).

It should by now be abundantly clear that Habermas's analysis of the rise and fall of the bourgeois public sphere is a powerful criticism of contemporary representative capitalist democracies. Indeed, *Structural Transformation* characterises them as

essentially illegitimate and corrupted. But it should also be apparent that from within this criticism springs hope, and the possibility of emancipation through the abstraction of the public sphere ideal from its specific and failed bourgeois incarnation. A vision of deliberative democracy emerges, within which legitimacy is conferred upon parliamentary proceedings through their steering by means of the rational-critically generated public opinion, generated in an egalitarian public sphere situated between the private and public realms, and free from state coercion and private inequalities.

This is the true value of *Structural Transformation*; that it provides a normative ideal or analytic category against which the realities of contemporary democracies can be measured, and the realisation of which can be striven towards. Fraser's claim that "no attempt to understand the limits of actually existing late-capitalist democracy can succeed without in some way or another making use of it" (1992: 111) is quite correct. How well the public sphere is functioning becomes "a concrete manifestation of society's democratic character and thus in a sense the most immediately visible indicator of our admittedly imperfect democracies" (Dahlgren 1991: 2). It is due to these qualities that *Structural Transformation* and the Habermasian concept of the public sphere continue to have resonance with the structures of contemporary society, and the reason for its continued importance and power as a text.

5.2 Habermas's 'linguistic turn'

This concern with generating a normative model of deliberative democracy continues within much of Habermas's later work. The reformulations and embellishments generated through this later work are often incorporated into an overall understanding of the 'Habermasian public sphere'. As such, a brief discussion of the main themes that emerge within the most notable of these subsequent texts is necessary for both our own understanding of the concept, and for the understanding of the body of criticism and revisionist modernisation that has

emerged around the author and his concepts. As Salter states, restricting discussion to just *Structural Transformation* and not Habermas's later work is a mistake (2003: 118). This work, while still focused on the concept of the public sphere and deliberative democracy, is distinguished by a significant and paradigmatic shift; Habermas's famous (or infamous) 'linguistic turn' towards a theory of communicative action. This theory presupposes that language itself contains norms that can criticise domination and foster democratisation.

Habermas saw the exercise of reason through rational-critical debate as "the valuable kernel in the flawed ideology of the bourgeois public sphere…" (Calhoun 1992: 2). The deliberative use of reasoned criticism is seen to result in an educated opinion, which is markedly different and infinitely more democratically legitimate than a vulgar aggregation of preferences constituted without deliberation (ibid.: 17). However, the over-pessimism of his own critical theory within *Structural Transformation* (which will be explored more fully in the following chapter) leaves no institutional basis with which to begin the democratising process, and no active subjects to work on, hence the vagueness and tentativeness of his conclusions (Kellner 2000: 10). As a result, he has come to believe that basing the theory of the public sphere on bourgeois liberal ideals and values is unsound, given the 'civilised barbarisms' of the twentieth century.

> When these bourgeois ideals are cashed in, when the consciousness turns cynical, the commitment to those norms and value orientations that the critique of ideology must presuppose for its appeal to find a hearing become defunct.
>
> (Habermas 1992: 422)

As such, Habermas's "inability to find in advanced capitalist societies an institutional basis for an effective political public sphere corresponding in character and function to that of early capitalism and state formation but corresponding in scale and participation to the realities of later capitalism and states" (Calhoun 1992: 30), has led him to seek an alternative and "deeper" basis for democracy (Habermas 1992: 422). His later work has found this "less historical, more transcendental

basis" in "an evolutionary account of human communicative capacity that stressed the potential implicit in all speech" (Calhoun 1992: 32). The theory of communicative action locates the basis for rational-critical deliberation not in institutional bases (as in the bourgeois public sphere) but in the transhistorical and dynamic communicative or rational capacities intrinsic to human communication. As such, "[t]he public sphere remains an ideal, but it becomes a contingent process of the evolution of communicative action, rather than its basis" (ibid.).

5.2.1 Lifeworld and system

He splits capitalist society into the categories of 'lifeworld' (constituted of personal relationships through to communicative action) and 'system' (the economy and the state, steered by money and administrative power). This dichotomy was initially introduced in *On the Logic of the Social Sciences* (1967) and *Legitimation Crisis* (1973), but only really came to full fruition in *The Theory of Communicative Action* (1987). The theme is then continued throughout his following work (most notably in *Between Facts and Norms* (1996)). The system is the domain of instrumental rationality, in which success is measured via the achievement of predefined goals, and governance is done by the 'steering imperatives' of money and power. The lifeworld, in contrast, is the domain of communicative rationality, aiming for understanding and consensus between individuals, secured by communicative actions free from manipulation, coercion, deception and strategy. The lifeworld is grounded in moral, aesthetic, practical and political considerations (Habermas, 1987: 304-5), and only it has a legitimate claim to the coordination of society, not the system.

However, the system is seen as constantly encroaching upon or 'colonising' the lifeworld, thus undermining its communicative rationality by imposing functional or instrumental rationality on lifeworld interactions through the system-steering imperatives of money and power (Habermas 1987). This colonisation involves extensions of state bureaucracies, legal regulation, political socialisation and

economic privatisation (Edwards 1992: 115). If it is allowed to succeed, then rational inter-citizen and citizen-state dialogue is replaced by "systemic and strategic exchanges of power. Citizens offer the state legitimacy (in the form of votes for parties and basic compliance with laws) in return for the benefits of the welfare state, whilst the state 'spends' its power in the form of the laws and policies it imposes on citizens; always mindful of the need to win votes" (Roberts & Crossley 2004: 8).

As such, the primary project for democracy is to protect the lifeworld from these systemic imperatives through the reassertion of communicative rationality against the state and economy's instrumental agendas. However, from the outset of his system/lifeworld distinction, Habermas has "considered the state apparatus and economy to be systematically integrated action fields that can no longer be transformed democratically from within… without damage to their proper system logic and therewith their ability to function." (1992: 444). The system cannot be altered, only kept in check. This is achieved through the exertion of communicative power generated by the public sphere against the system, achieving a permanent, democratically healthy equilibrium between communicative and instrumental rationality.

This "[c]ommunicative power is exercised in the manner of a siege. It influences the premises of judgment and decision-making in the political system, without intending to conquer the system itself." (Habermas 1996: 486). This siege or "democratic dam" must ensure that communicative power can prevail over the steering imperatives of money and administrative power and therefore "successfully assert the practically oriented demands of the lifeworld" (Froomkin 2004: 424).

Elections are now seen as an important part of this articulation: "Informal public opinion-formation generates 'influence'; influence is transformed into 'communicative power' through the channels of political elections; and communicative power is again transformed into 'administrative power' through legislation" (Habermas 1996: 28). This shifts public sovereignty:

> …into a flow of communication… in the power of public discourses that uncover topics of relevance to all society, interpret values, contribute to the resolution of problems, generate good reasons and debunk bad ones. Of course, these opinions must be given shape in the form of decisions by democratically constituted decision-making bodies. The responsibility for practically consequential decisions must be based in an institution. Discourses do not govern. They generate a communicative power that cannot take the place of administration… but can only influence it. This influence is limited to the procurement and withdrawal of legitimation.
>
> (Habermas 1992: 452)

The public sphere generating the public opinion and hence communicative action is later theorised in *Between Facts and Norms* (1996) as having a 'core' administrative complex, governed by rules and capable of action, and a 'periphery', which is the social space constituted through communicative action. Issues and deliberation work their way through from the periphery to the core. This public sphere must be grounded in a civil society composed of "those non-governmental and non-economic connections and voluntary associations that anchor the communicative structures of the public sphere in the society component of the lifeworld" (Habermas 1996: 66-67). 'New' or non-class-based social movements, seen as arising in response to conflicts at the "seam between the system and the lifeworld", are considered an important component of this grounding (Habermas 1981: 36). The public sphere amplifies problems situated in the lifeworld, and "can best be described as a network for communicating information and points of view" (ibid.: 360).

We can begin to see how this understanding of the public sphere has resonance with hacktivism, which does not intend to seize control of any administrative role within the system, but instead exerts influence from the periphery of the lifeworld. Hacktivist discourses "do not govern", but they aim to generate fields and flows of 'communicative power' that both inform and come to constitute the wider public's (or publics') 'procurement and withdrawal of legitimation' through such mechanisms as voting. However, hacktivism transgresses the procedural constraints that Habermas sees as necessary to confer legitimacy upon the deliberative generation of this communicative power.

5.2.2 Procedural constraints and communicative legitimacy

The legitimacy of the communicative action or power conducting the siege against system colonisation is conferred via the process of deliberation within the public sphere, which must, as far as possible, approach an ideal speech situation. In a general sense, participants in the deliberation must come as close as possible to an ideal situation in which:

> …(1) all voices in any way relevant get a hearing, (2) the best arguments available to us given our present state of knowledge are brought to bear, and (3) only the unforced force of the better argument determines the 'yes' and 'no' responses of the participants.
>
> (Habermas 1996: 13)

Clearly, Habermas's theory of communicative action both extends organically from *Structural Transformation* in that it continues his concern with the rational-critical public sphere and deliberative democracy, but also departs markedly from this previous text, in that the public sphere ideal and deliberative democracy he now advocates are not so much institutionally but strongly procedurally based. Rational consensus is not ensured via the limiting of the scope and content of deliberation, but through the procedural constraints of the ideal speech situation. These procedures will 'weed out' illegitimate and inferior discursive positions.

Dahlberg (2004: 29-30) provides a concise and exact summary of these procedural features, taken from several Habermasian texts (1984: 1-26; 1990: 43-115; 1993: 31-33, 56-76; 1996: 267-387; 2001):

1. *Thematisation and reasoned critique of problematic validity claims*… the positions put forward and the subsequent questioning are backed by reasons.

2. *Reflexivity*. Participants critically examine their values, assumptions, and interests, as well as the larger social context.

3. *Ideal role taking.* Participants attempt to understand the argument from the other's perspective. This involves empathetic listening, which in turn means a commitment to an ongoing dialogue with difference.

4. *Sincerity.* Deliberation is premised upon honesty or discursive openness in contrast to deception, including self-deception for which one must remain 'critically alert". Further, rational judgement presupposes that participants make a sincere effort to make known all relevant information, including their intention, interests, needs and desires.

5. *Inclusion and discursive equality.* Debate is open to all those affected by the concerns under consideration, and each participant has an equal opportunity to introduce and question any assertion whatsoever and to express attitudes, desires and needs.

6. *Autonomy from state and economic power.* Deliberation is driven by the concerns of publicly oriented citizens rather than by money or administrative power.

5.2.3 Conclusion

Habermas's later conception of the public sphere thus retains the basic ideal of the old – that participants bracket their private selves in order to deliberate rationally as equals on matters of common or public interest, in order to secure a legitimate consensus on what will best serve the common good. However, instead of being constituted through the institutions of the press or public meetings, the public sphere arises wherever the normative procedures of communication are instituted and an ideal speech situation arises. Both former and latter conceptions have been criticised and reformulated individually, and sometimes in combination, from a wide range of perspectives. It is this fertile diversity of criticism that we will now investigate – moving past Habermas's selectively-understood histories and the

problematic procedural constraints that would render hacktivism an illegitimate form of communicative power generation, and exploring how we might enable the theory of the public sphere to wander through "wider and wilder territory" (Ryan 1992: 286).

Chapter 6

The neo-Habermasian public sphere

Despite the clear value of Habermas's public sphere theory, or perhaps more accurately, because of it, there are and have been multiple criticisms leveled at Habermas and *Structural Transformation*, and his continuation of its themes within later work. Indeed, "[f]ew books have been so systematically discussed, criticised and debated, or inspired so much theoretical and historical analysis" (Kellner 2000: 7). However, as Fraser has stated, "the public sphere theory is in principle an important critical-conceptual response that should be reconstructed rather than jettisoned, if possible" (2005: 2). Calhoun concurs: "The most important destiny of Habermas's first book may prove to be this: not to stand as an authoritative statement but to be an immensely fruitful generator of new research, analysis, and theory… an indispensable point of theoretical departure. It should also continue to inform a rich tradition of empirical work" (1992: 41).

Indeed, there is little point in simply accepting Habermas's conclusions, both pre- or post-linguistic turn – society remains constantly dynamic, hence the public sphere within it must be equally continually re-examined (Dahlgren 1991: 2). An investigation of these criticisms and recontextualisations leads to a modernisation and reformulation of the public sphere ideal, which much more adequately deals with issues of power, exclusion and difference. This 'neo-Habermasian' public sphere is also much more applicable and appropriate to the current social environment, and hence more useful to the investigation of the practice of hacktivism.

6.1 Historical inaccuracies within the bourgeois public sphere: Practical criticisms

One of the most fundamental criticisms leveled at *Structural Transformation* is that Habermas's assessment of the historical bourgeois public sphere is over-idealistic, seemingly to the point of naïveté or ignorance (Calhoun 1992; Curran 1991; Dahlgren 1991; Eley 1992; Fraser 1992; Garnham 1992; Golding 1995; Kellner 2000; Negt & Kluge 1992; Roberts & Crossley 2004; Ryan 1992; Thompson 1993). Although he does assert in his introduction to *Structural Transformation* that his investigation "presents a stylised picture of the liberal elements of the bourgeois public sphere" (1989: xix), criticisms regarding the extent of this stylisation are, nonetheless, well founded. The values of the bourgeois public sphere are abstracted into a public sphere ideal, thus it is important that they be based upon reasonably accurate observations, or at the very least, observations that are explicitly aware of any lionising and contradictory tendencies within themselves. Curran contends that Habermas's analysis is deeply flawed in that "it is based on contrasting a golden era that never existed with an equally misleading representation of present times as a dystopia" (1991: 46).

As such, there are four main critical assertions leveled: that Habermas over-idealised the internal function of the bourgeois public sphere; that he ignored the existence of multiple historical public spheres, that he did not adequately and fully acknowledge the exclusion inherent to the bourgeois public sphere; and that his analysis of the contemporary media and public sphere is unnecessarily and unproductively pessimistic.

6.1.1 An over-idealisation of the internal function of the bourgeois public sphere

The first of these is that the bourgeois public sphere (especially in terms of its institutional basis is the press) was not nearly as internally rational-critical as Habermas claims (Calhoun 1992; Curran 1991; Eley 1992; Garnham 1992; Golding 1995; Kellner 2000). The bourgeois press, rather than being an impartial domain governed by the force of the better argument and free from state control, was in fact rife with corruption and factions, and never broke completely free from political influence (Curran 1991: 41). In addition, Golding claims that the press emancipation from state control that did occur was less the result of a heroic battle for the freedom of ideas and more to do with the press's growing commercial viability (1995: 27). Habermas also ignores the non-rational-critical elements of the bourgeois press, such as 'penny dreadfuls' and scandal sheets (Calhoun 1992: 33). "This refutes the contrast made by Habermas between the early press as an extension of rational-critical debate among private citizens, and the later press as the manipulative agency of collectivised politics" (ibid.: 41-42). Furthermore, he disregards the radical press of the times as non-rational, when in fact, they were merely challenging the bourgeois status quo of the mainstream press and public sphere, in an attempt to articulate the positions of the proletariat (ibid.: 41). At this most basic of historical levels, we can begin to see the Habermasian tendency to overlook the true extent of the institutionalisation and normalization of exclusion, and, indeed, collude in the theoretical marginalization of alternative publicity.

6.1.2 The existence of multiple historical public spheres

This feeds directly into the second major historical criticism; that Habermas completely and inexcusably ignores a number of alternative public *spheres* that

were simultaneously present in society, choosing instead to assert that the unitary Westphalian-national bourgeois public sphere was *the* public sphere (Curran 1991; Dahlgren 1991; Eley 1992; Fraser 1992; Garnham 1992; Golding 1995; Negt & Kluge, 1992; Ryan 1992; Thompson 1993). He fails to acknowledge the presence of a number of alternative, plebeian, popular, informal or oppositional public spheres (Dahlgren 1991: 6), seeing them only as late developments signaling the demise of the public sphere proper (Fraser 1992: 122). Habermas has since acknowledged this flaw (1992: 424-427) but this basic criticism of *Structural Transformation* must nonetheless be noted as it has led to major theoretical revisions within the field, many of which prove to be integrally relevant to a public sphere theoretical conceptualisation of hacktivism.

Negt & Kluge were the first to begin this critical project with the 1972 publication of *Öffentlichkeit und Erfahrung: Zur Organisationsanalyse von Bürgerlicher und Proletarischer Öffentlichkeit* (Public Sphere and Experience: Toward an Analysis of the Bourgeois and Proletarian Public Sphere), their nationality giving them a jumpstart on English academics. The translation of this text was published in 1993, giving the English-speaking world a somewhat belated full access to their criticism of Habermas for not acknowledging the existence of plebeian and proletarian public spheres. With regards to this text, one tends to agree with Downing, that there is "a strongly doctrinaire and abstractly utopian character to large parts of their argument" but that it is nevertheless important in questioning the concept of a unitary public sphere (2001: 29)

Eley (1992) provides a further examination of non-bourgeois public spheres. Although Habermas did acknowledge *a* plebeian public sphere, he saw it as merely a suppressed variant of the bourgeois version (Habermas 1989: xviii). This dismissal does not seem at all warranted, and seemingly served only to maintain the integrity of Habermas's argumentative thrust. For, as Eley explains, the presence of the plebeian public sphere illustrates that public spheres could arise from diverse origins: "The virtue of publicness could materialise other than by the intellectual transactions of a polite and literate bourgeois milieu" (Eley 1991: 304). Ryan (1992) contributes to this discussion by detailing the existence of multiple nineteenth century American public spheres that combined rational-critical debate

with more rambunctious and conflictual behaviour. Her discussion is set within a feminist interpretation of public sphere theory, more of which will be discussed shortly.

Furthermore, the aforementioned radical press constituted a highly literate and combative public sphere; hence, rational-critical debate was not the exclusive domain of the bourgeois (Eley 1991: 304-305). Eley also asserts that due to the international impact of the French revolution, public spheres arose all through Europe via conscious efforts on behalf of the citizenry in more "backwards" nations in an attempt to articulate their aspirations, rather than as the result of prior social development (ibid.: 305). Eley's underlying point is that by idealising the bourgeois public sphere and ignoring other forms, Habermas "misses the extent to which the public sphere was always constituted by conflict" (ibid.: 306), an assertion which has clear resonance with the subversive and provocative practice of hacktivism, and which is explored in further detail in the next category of criticism.

6.1.3 Unacknowledged exclusions from the bourgeois public sphere

The third criticism is integrally linked to the former two – that entry into the historical bourgeois public sphere was significantly more exclusive than Habermas acknowledged. Habermas tends to speak of the confluence between *bourgeois* and *homme* that governed class exclusions within the public sphere as an essentially un-premeditated condition arising from the societal structures of the time. He briefly discusses the ideological nature of this conflation in his engagement with Marx, but this aspect is, for the most part, glossed over by his idealisation of the bourgeois public sphere. This failure to attend to intentional exclusions has since been extensively criticised. Furthermore, it is also argued that not only did exclusions arise along the axis of class, but along those of gender as well, in a similarly premeditated and systemic manner.

6.1.3.1 Class-Based Exclusions

Habermas has been repeatedly criticised for failing to adequately acknowledge the fact that the bourgeois public sphere was not only oriented towards defending civil society from the state, but also towards the production of power relations within civil society and the repression of non-bourgeois strata (Calhoun 1992: 39; see also Curran 1991; Eley 1992; Fraser 1992; Golding 1995; Roberts & Crossley 2004). It is true that he does go some way towards acknowledging this fact, but "not to the extent of compromising his basic historical claim" (Eley 1992: 293) and thus his conception of the public sphere. Given the recognition that there were multiple forms of competing publics, the conflation of *bourgeois* with *homme* no longer seems accidental – it seems more a way of "defining an emergent elite, of setting it off from the older aristocratic elites it was intent on displacing on the one hand and from the various popular and plebeian strata it aspired to rule on the other" (Fraser, 1992: 114).

In particular, the rationality of the bourgeois press has been questioned, with Curran claiming "the newspapers celebrated by Habermas were engines of propaganda for the bourgeoisie rather then the embodiment of disinterested rationality" (1991: 40). Eley (1992) draws a Gramscian conclusion from this account: that the rise of the bourgeois public sphere marked a shift from a force-based era of rule to one characterised by consent elicited through more subtle repression. "The official public sphere, then, was, and indeed is, the prime institutional site for the construction of the consent that defines the new, hegemonic mode of domination" (Fraser 1992: 117). As such, we should follow Fraser's lead in seeking ways to conceive of contestation of this hegemony, in terms of both theory and praxis (which is one of the central aims of this thesis and its focus on hacktivism). Through Habermas's characterisation of class-based exclusion from the bourgeois public sphere as essentially innocent of purposive power play, he ignores the way in which rational-critical communication is founded on intentional exclusions and repression (Roberts & Crossley 2004: 11). This point re-emerges in the discussion of further, more theoretical criticism.

6.1.3.2 Gender-based exclusions

As noted, *Structural Transformation* does go some way towards recognising class exclusion, which is more than can be said of its treatment of exclusions based on gender. Numerous critics (Calhoun 1992; Dahlgren 1991; Eley 1992; Fraser 1992; Garnham 1992; Landes 1988; Ryan 1992; Thompson 1993) have identified a systemic exclusion of women from the bourgeois public sphere, proving the starting point for a body of feminist public sphere theory, and undermining the sharp distinction between public and private that provides the basis for the public sphere ideal conceived in *Structural Transformation*. Habermas does go some way towards accepting these criticisms in his later work (1992), but not far enough to resolve the structural instabilities they highlight. As Calhoun says, this failure is typical of a general "thinness of attention to matters of culture and the construction of identity" within Habermas's work on the public sphere and deliberative democracy (Calhoun 1992: 34).

The literature of Fraser, Eley and Ryan provides the sharpest insight into this issue. All three locate the "structural underpinnings of gender inequality along the private-public axis" (Ryan 1992: 260), in that "the same structural transformation that gave definition to a public realm designated women a second species of citizens and marked out around them a social space called the private" (ibid.: 67). In the eighteenth century, as part and parcel of the association of rationality with the public sphere, as opposed to the private world of the family and economics, femininity came to be associated with the private realm, and masculinity with the public. "The new category of the "public man" and "his "virtue" was constructed via a series of oppositions to "femininity", which both mobilised older conceptions of domesticity and women's place and rationalised them into a formal claim concerning women's "nature"" (Eley 1992: 309). The very constitution of the bourgeois public sphere was based on this gender-ideological dichotomy.

Habermas's view of the bourgeois public sphere as *the* public sphere, and the emphasis implicitly placed upon the superiority of a singular public sphere, is thus exposed as even more ideological. As Ryan shows through her assessment of

eighteenth and nineteenth century American political life, there was in fact a range of highly inventive female public spheres in existence, which arose in response to this systematic exclusion from the mainstream. The reality of multiple and competing publics is once again brought to light, underlining the need for any reconceptualization of the public sphere to allow for the existence of multiple contestatory publics arising in response to exclusion from or opposition to the 'mainstream' or dominant public.

Furthermore, this structured gender exclusion was not the exclusive domain of the bourgeois. The same occurred within the plebeian and radical public spheres, due to the new capitalist regime forcing women and children out of the home and into the workplace in order to help support the family. This undermined the masculine role of patriarch and breadwinner, and was seen as upsetting the natural order. The desire to keep women 'in their place' was thus linked to economic desires and anxieties, and resulted in a reassertion of masculinity as linked to publicness within the working classes as well (Eley 1992: 314-316). Ryan's identification of both bourgeois and working class American female public spheres corroborates the multi-class character of this phenomenon.

6.1.4 An over-pessimistic analysis of the contemporary media and public sphere

We have covered Habermas's "over-rosy portrayal of the emergence and early character of the public sphere"; now we must address his "unduly pessimistic characterisation of the present" (Golding 1995: 28). Criticism has been leveled at Habermas's gloomy view of the contemporary media and public sphere, and lack of attention to audience or citizen activity and agency (Calhoun 1992; Curran 1991; Dahlgren 1991; Garnham 1992; Golding 1995; Kellner 2000; Roberts & Crossley 2004; Thompson 1993). As Dahlgren says, "while we cannot ignore the dominance of the mainstream media, we should be careful not to exaggerate unnecessarily their

homogeneity or monolithic character", lest our pessimism become crushing rather than inspiring, and leave us apathetic or paralysed (1991: 9). Habermas is arguably guilty of exactly this. His characterisation of the modern electronic media as stultifying and hypnotic is completely untempered by any attention to audience agency. Citizens are seen as passive dupes, a perspective that has been refuted by a large body of research into active audience theory (Curran 1991: 42). This tendency is a clear product of his Frankfurt School background.

Promisingly, Habermas does acknowledge this deficiency in later work: "[M]y diagnosis of a unilinear development from a politically active public to one withdrawn into a bad privacy, from a 'culture-debating to a culture-consuming public', is too simplistic. At the time, I was too pessimistic about the resisting power and above all the critical potential of a pluralistic, internally much differentiated mass public whose cultural usages have begun to shake off the constraints of class" (Habermas 1992: 438). However, his work in *Beyond Facts and Norms* (1996) exhibits a return to the idea that the mass media are a hopelessly negative influence on the public sphere, as do his more recent articles (for example, Habermas 1996) and he "does not discuss the normative character of communication media in democracy or suggest how a progressive media politics could evolve" (Kellner 2000: 15). Kellner suggests that his idealisation of print media and denigration of electronic media may stem from the fact that he is simply more familiar with, and is much more firmly ensconced within the world of letters. Whatever the reason, there is no doubt that this totalising disparagement of non-print media is neither accurate nor useful.

In relation to this, he has also done very little work in accounting for the rise of the Internet – his idea of electronic media remains largely confined to broadcasting technologies. While we must bear in mind that he is of advanced age and is no longer as prolific as he once was, this is nonetheless a serious inadequacy. While the hyperbolic laudation of the Internet as a technology currently overthrowing the old world order and replacing it with a new democratic era is to be avoided, there is no doubt that it has enabled new forms of organisation and communication that do have significant democratic value. Yet Habermas has only addressed the capabilities in a glancing and dismissive fashion.

The publication of his keynote speech to the 2006 International Communication Conference provides some insight into his opinion of the Internet (Habermas 2006), but this brief mention is in an endnote – the very placement of it suggests extreme disregard. In this self-categorised 'passing remark', he claims that the only democratic benefit of the Internet is that it "can undermine the censorship of authoritarian regimes that try to control and repress public opinion" (ibid.: 423). He categorises all other online communication claiming democratic value as "parasitical" and "fragmented" – online debates only promote political communication through "crystallizing around the focal points of the quality press", and chat rooms and their ilk "lead to the fragmentation of large but politically focused mass audiences into a huge number of isolated issue publics." The examples he uses to make these points are specific and unrepresentative, thus undermining his general conclusions, and his claims of fragmentation completely ignore the multiple issue or community 'belongings' and extensive issue and interest interconnections facilitated and even extended by the Internet. As Bruns summarises:

> Habermas's obvious aversion to accepting the Internet as part of the public sphere, or (more to the point) to modifying the public sphere model for the network age, is as inexplicable as it is unfortunate; with Net-based communication now a staple of everyday discussion, debate, and deliberation on political as well as virtually all other topics, it serves only to undermine the public sphere concept itself. As responses even to the limited references to the Internet in his ICA speech show, Habermasians are clearly hanging out for a more considered approach to addressing the question of incorporating the Net into the public sphere model…
>
> (Bruns 2007)

In the complex and populous modern world, the media and media platforms such as the Internet are necessarily the main platform for public spheres, and a subtler and less dogmatic approach is necessary in order to unravel their true significance and scope within this role. Indeed, the theorisation of a public sphere model that allows for these new technologies and that recognises an active and participatory citizenry

is the primary intent of this thesis, with hacktivism providing a specific portal into the ways in which active and engaged citizens can generate much more 'communicative power' online than Habermas gives them credit for, as well as avoiding the isolation and cyberbalkanization that he seems to regard as so inevitable.

6.2 Theoretical criticisms and reformulations

Clearly, the Habermasian public sphere has been roundly criticised on grounds of historical inaccuracies, but there is also a large body of literature criticising the more abstract theory of the public sphere ideal Habermas extracts from *Structural Transformation* and his later work. Some of this feeds off historical criticisms, some arises independently, and much leads to innovative new reformulations of the public sphere concept. As stated in the introduction to this section, the networked nature of the responses to Habermas's work requires laying one's allegiance with a particular strand of thought in the interests of argumentative cohesion and strength. The school of thought seen as the most legitimate and thus adopted and discussed has been variously described as 'postmodern' (Roberts & Crossley 2004: 14), 'poststructuralist', 'agonistic' (Dahlberg 2007a), and 'radical' (Dahlberg 2007b), and also exhibits a strong feminist component. All these labels are appropriate, but the core of what defines this theoretical strand hinges upon its treatment of power and difference.

While agreeing with the underlying principles of the Habermasian public sphere and the deliberative theory of democracy it espouses, the Habermasian treatment of underlying societal power structures is seen as totally inadequate. In order to effectively deal with these issues, a new theoretical conception based around the notions of multiple public spheres, discursive contestation, a deeper engagement with identity and difference, and an expansion of legitimate forms of debate must be hypothesized. To achieve this, the public/private dichotomy underlying the Habermasian public sphere is questioned, as is the focus on exclusively rational-

critical deliberation intended to secure a consensus on matters of common interest. Given that this field of theory combines aspects of all its proposed titles – radicalism, agonism, postmodernism, poststructuralism – none of these titles, on their own, seem particularly appropriate. As such, the admittedly highly non-descriptive moniker of 'neo-Habermasian public sphere theory' will be used. There are, of course, multiple instances of what could legitimately be called 'neo-Habermasian' conceptions of the public sphere, but within this text, the term will be used to describe the intersections of the literature about to be discussed.

6.2.1 Nancy Fraser and 'Rethinking the Public Sphere'

The critical feminist Nancy Fraser is arguably the 'mother' of neo-Habermasian public sphere theory. In 'Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy' (1992), a mere three years after *Structural Transformation* was published in English, she laid out the solid foundations upon which a host of other theorists have built. In it, she recognises the public sphere as an "indispensable resource" for democratic theory (1992: 109), but contends that "the specific form in which Habermas has elaborated this idea is not wholly satisfactory" (ibid.: 111). Drawing upon the alternative histories of Landes, Ryan and Eley (1988; 1992; 1992; respectively), and the previously discussed historical criticisms that they inform, Fraser attempts to answer the consequential question of whether the Habermasian public sphere is best seen as "an instrument of domination or a utopian ideal" (Fraser 1992: 117). Her answer is that it is neither; it is a valuable concept that is simply predicated on erroneous assumptions, and as such should be "reconstructed rather than jettisoned" (ibid.: 2). This 'call to action' is the critical engine of this thesis, and her theory provides the backbone for the generation of the neo-Habermasian framework.

6.2.1.1 The impossibility of bracketing status differentials

The first of these erroneous assumptions is that it is possible for participants in the public sphere to 'bracket' their private status differentials. As discussed, the bourgeois public sphere was effectively closed to the proletariat and women, as well as racial minorities. However, Fraser argues that even if perfect formal access had been ensured, informal inequalities would have persisted due to the impossibility of the idea of status bracketing. Inequalities were ingrained within the very fabric of the rational-critical debate privileged within the bourgeois public sphere, in that "discursive interaction within the bourgeois public sphere was governed by protocols of style and decorum that were themselves correlates and markers of status inequality." (ibid.: 119). That is, the rational-critical mode of speech was the domain of the bourgeois male, and as such, would have given them an immediate advantage within deliberations with non-bourgeois non-males.

Fraser argues that this inequality persists in contemporary relations between sexes: even though women are now granted access to public deliberation, they tend to be disadvantaged due to the propensity for men to be more aggressive and prolonged speakers. This gender inequality can be generalised into racial and ethnic inequality, in that minorities may frequently find that they lack the 'legitimate' mode of speech, and as such, are marginalised in public discourse. An insistence upon the bracketing of social inequalities within public discourse is, therefore, counterproductive. Rather than creating a 'level playing field', it generally "works to the advantage of dominant groups in society and to the disadvantage of subordinates" (ibid.: 120). Furthermore, contemporary political economy, and in particular, the corporate and mediated public sphere, means that those discursively subordinate groups also tend to lack access to the means of participation – as do other, varied minority or alternative sub-populations. "[P]olitical economy enforces structurally what culture accomplished informally" (ibid.). As such, bracketing is nigh on impossible when deliberation occurs with arenas "pervaded by structural relations of dominance and subordination" (ibid.). The comprehensive 'unbracketing' of private status would work towards more equal deliberation, but

the only way equality could truly be ensured is through the total elimination of systemic social inequalities (ibid.: 121).

6.2.1.2 The value of multiple public spheres: The birth of the counterpublic

The second Habermasian assumption questioned by Fraser is that having one overarching public sphere is good for democracy, while having a multiplicity of smaller spheres is not. This assumption is revealed through Habermas's interpretation of the emergence of multiple smaller publics as heralding the decline of the public sphere as such. Yet, given the deep and structured stratification of society, and the impossibility of bracketing status differentials within deliberation, a theory that accommodates "contestation among a plurality of competing publics" is infinitely preferable (ibid.: 122). A plurality of "subaltern counterpublics" is needed; "parallel discursive arenas where members of subordinated social groups invent and circulate counterdiscourses to formulate oppositional interpretations of their identities, interests, and needs" (ibid.: 123). Fraser's elucidation of this idea has firmly established the notion of counterpublicity as an integral component to any modern conceptualisation of the public sphere. Counterpublics provide subordinated groups with spaces in which to hone their deliberative skills, by deliberating on their own needs in an arena free from elite supervision. Once they have attained adequate deliberative power, they can engage with other counter- or dominant publics, and more successfully oppose continued subordination (ibid.). This opposition may entail both deliberation and more direct forms of contestation – an extremely significant advance on Habermas's strict procedural constraints, and one that is central to public sphere theoretical interpretation of hacktivism.

Fraser makes it clear that counterpublics, despite being explicitly oriented against domination and towards the expansion of discursive space, are not necessarily "virtuous" – various right-wing causes provide clear illustration of this. We may

not agree with all counterpublics; they may not be 'pretty' – but their existence and recognition is, nonetheless, tremendously valuable. This is certainly the case with hacktivism – we may not always agree with hacktivists' causes or even their methods and conduct, but this does not mean that they have no democratic legitimacy. Pluralist democracy in action is an inherently messy and conflictual process, as is presently made abundantly clear through a discussion of Chantal Mouffe's agonistic public sphere thesis.

However, Fraser also pre-empts the accusation that counterpublics tends towards being separatist enclaves, asserting that all true publics are predicated on the intent to increasingly broaden the circulation of their discourse. Hence, subaltern counterpublics are doubly significant: "On the one hand, they function as spaces of withdrawal and regroupment; on the other hand, they also function as bases and training grounds for agitational activities directed towards wider publics" (ibid.: 124). Their ability to offset gaps in 'participatory parity' stems from the relationship between these two functions. Furthermore, because the very definition of a public relies on its members being diverse in some way, internal reification is limited, and citizens may potentially belong to multiple publics (ibid.: 127). In addition, the fact that public spheres not only construct public opinion, but are also "arenas for the formation and enactment of social identities" (ibid.: 125) is acknowledged.

This identification of the dual internal and external functions of publics and counterpublics is an important structural component of this thesis, in that it focuses on the external activities of hacktivist groups rather than their internal cohesion- and solidarity-making efforts, which have been previously explored by such scholars as Samuel. Her internal typology provides the basis for the case study sampling, but these studies then focus on the externally-oriented publicity work done by the groups in question. The issues of incomplete internal reification and participation in multiple simultaneous publics also emerge as important issues within the public sphere theoretical investigation of hacktivism undertaken in this researcb.

6.2.1.3 Questioning the barrier between public and private

The third erroneous Habermasian assumption is that public deliberation should always be oriented exclusively towards the public good, at the expense of private interests. Fraser interrogates these terms, and comes to the conclusion that the boundary between the public and the private realms is dynamic, and interpreted differently by various individuals and groups. The definition of exactly which issues are of concern to everyone is as needy of deliberation as the final decision made regarding each issue. Therefore, truly democratic public deliberation requires "positive guarantees of opportunities for minorities to convince others that what in the past was not public in the sense of being a matter of common concern should now become so" (ibid.; 129). This ability to mobilise public attention towards and deliberation upon what would otherwise be non-publicly examined issues is yet another significant facet of hacktivist activity.

Furthermore, the existence of a consensus regarding the common good cannot be presumed in advance – sometimes one will emerge, and other times, not. Judgments about just what is and is not open for discussion cannot be made in advance of deliberation. As such, within our stratified society, "any consensus that purports to represent the common good… should be regarded with suspicion, since this consensus will have been reached though deliberative processes tainted by the effects of dominance and subordination" (ibid.: 131). The idea of a 'common good' masks the actuality of a 'dominant good'. Fraser thus exposes the terms 'private' and 'public' as ideological, in that they may be used to "delegitimate some interests, views, and topics and to valorise others" (ibid.).

6.2.1.4 Questioning the separation of the public sphere(s) from the state

The final Habermasian assumption problematised by Fraser is his insistence that a functioning public sphere requires a clear separation between civil society and the state. If 'civil society' is interpreted as a nexus of non-governmental, non-economic, and non-administrative associations, then it certainly should be kept separate from the state in order to protect the autonomy of the public spheres. But the problem with this is that it renders the public spheres 'weak' in the Barber-esque sense (1984; 1998), in that they have no decision-making powers. The question is then how accountable the 'strong' publics of the parliament are to the 'weak' public spheres, and how this accountability can best be fostered. Fraser has no real answers to this, but it is clear that any formulation of the public sphere that assumes a strict demarcation between civil society and the state is "unable to imagine the forms of self-management, interpublic coordination, and political accountability that are essential to a democratic and egalitarian society" (ibid.: 134).

Fraser (1995) somewhat abandons this fourth concern, but, significantly, identifies her strand of public sphere theory as postmodern, in opposition to the modernism of Habermas (1995: 288). She also provides a useful summation of the requisite characteristics for any postmodern theory of the public sphere:

> a) A postmodern conception of the public sphere must acknowledge that participatory parity requires not merely the bracketing, but rather the elimination, of systemic social inequalities;
>
> b) Where such inequality persists, however, a postmodern multiplicity of mutually contestatory publics is preferable to a single modern public sphere oriented solely to deliberation;
>
> c) A postmodern conception of the public sphere must countenance not the exclusion, but the inclusion of interests and issues that bourgeois masculinist ideology labels 'private' and treats as inadmissible.
>
> (Fraser 1995: 295)

6.2.2 Beyond Fraser

Fraser provides an invaluable springboard for further thinking about the postmodernisation or radicalisation of public sphere theory. As such, her theoretical revisions provide a useful framework with which to explore the rest of this field, and they structure the following section, which reiterates, advances and refines her core assertions.

6.2.2.1 Multiple public spheres

6.2.2.1.1 The concept of the counterpublic

As previously mentioned, there has been widespread support for and continuation of Fraser's theme of the importance of counterpublics[23] (Benhabib 1996; Butsch 2007; Calhoun 1992, 1997; Crossley, 2004; Dahlberg 2007, 2007a, 2007b; Downey 2007; Downey & Fenton 2002, 2003; Downing 2007; Dryzek 2000, 2001; Eley 1992; Fraser, 2005; Kahn & Kellner 2004, 2005; Keane 2000; Kowal 2002; McLaughlin 2002; Poster 2001; Robbins 1993; Roberts & Crossley 2004; Ryan 1992; Schiller 2007; Warner 2002).

Fraser's peers, Eley and Ryan (both 1992) both provide historical evidence to support the contention that the concept of multiple publics was both far more factual and much more useful in terms of the acknowledgment and management of

[23] It is worth noting that Negt & Kluge did actually posit this idea 20 years earlier in the German publication of *Public Sphere and Experience: Toward an Analysis of the Bourgeois and Proletarian Public Sphere* (1972). However, this text, both because of its 20-year delay in being translated into English, and the fact that Fraser's counterpublic sphere theory is significantly more grounded and powerful, is much less frequently referenced within the counterpublic sphere tradition. It is probably also worth mention that there is, apparently, a large body of literature on the public sphere in the German language. For literacy reasons, this remains inaccessible.

ingrained and systemic societal power differentials. However, Eley not only provided historical fuel for Fraser's theory, he also identified the way in which Gramsci's argument that hegemonic projects were strongly centred not just in state-citizen dealings, but *within* civil society as well, could be analogised into multiple or counterpublic sphere theory. Dominant groups do not only exert their power through state functions, but in a more pervasive and subtle manner within civil society – the commercial media oligarchy being a prime example of this hegemonic function. The goal is to articulate their own conceptions of the world in such a way that they appear and become normative, while simultaneously engaging in the project of neutralising rather than explicitly suppressing opposing perspectives. However, any hegemonic project is necessarily ongoing, in that it is based within a pluralistic society stratified by class relations (Eley 1992: 323), thus providing conceptual room for the fracturing or threatening of hegemony.

Indeed, hegemony is never definitely secured or static, and is always open to contestation. "The dominance of a given social group has to be constantly renegotiated in accordance with the fluctuating economic, cultural, and political strengths of the subordinate classes" (ibid.: 324). Eley saw this renegotiation as occurring within the mainstream or dominant public sphere, with counterpublic spheres functioning as counterhegemonic projects, constantly contesting and eroding the stability of the dominant or hegemonic sphere. Eley thus contributes significantly to neo-Habermasian public sphere theory, not just by highlighting historical inaccuracies within *Structural Transformation*, but by also identifying ways in which the concept of the Habermasian public sphere needs to be "clarified and extended" in order to properly grasp hegemonic power relations (Eley 1992: 331). In line with this argument, the reconceptualization of public sphere theory to allow for an exploration of the ways in which hacktivists generate counterhegemonic projects is a core goal of this thesis.

Like Eley, Downey & Fenton believe that "[c]ounter public spheres may provide vital sources of information and experience that are contrary to or at least, in addition to the dominant public sphere thereby offering a vital input to democracy" (2002: 10-11). Their contention that counterpublic spheres tend to emerge predominantly in response to crises in the dominant public sphere links in with

Eley's discussion of hegemony, in that counterpublics functioning in a counterhegemonic manner are likely to be able to establish a firmer grounding and presence within cracks in the façade of the dominant public spheres' hegemonic project. "When the dominant public sphere is felt to betray or is no longer capable of allowing for critical rational engagement then trust is diminished allowing counter public spheres the opportunity to flourish" (ibid.: 9).

Warner reiterates this relationship between multiple publics, power differentials, and ideological or hegemonic struggle, stating that "some publics are more likely than others to stand in for *the* public, to frame their address as the universal discussion for the people" (2002: 117). Thus the importance of counterpublics is their ability to and orientation towards "actively and effectively contest[ing] the discursive boundaries of the mainstream public sphere" (Dahlberg 2007a: 57).

Downey and Fenton later make it clear (2003) that this interpretation is drawn from a shift within Habermas's work, from seeing the public sphere at rest towards seeing it in a constant state of flux (Habermas 1996). He postulates that when civil society groups mobilise to bring concerns from the periphery of the public sphere towards the centre, "the structures that actually support the authority of a critically engaged public begin to vibrate. The balance of power between civil society and the political system then shifts" (ibid.: 379). Again, this can be seen in terms of an ongoing hegemonic struggle.

However, Downey & Fenton make the point that no counterpublic can escape the context of existing "industrial-commercial" public spheres; indeed, the very term 'counterpublic' implies that their orientation is towards challenge as opposed to complete escape (Downey & Fenton 2003: 193). Again, Warner's treatment of this issue is similar: "A counterpublic maintains at some level, conscious or not, an awareness of its subordinate status. The cultural horizon against which it marks itself off is not just a general or wider public but a dominant one" (2002: 119). As such, a degree of interaction with the mainstream media is seen as an almost unavoidable component of successful counterpublic strategising (Downey & Fenton 2003: 193).

Echoing Fraser, they reassert the fact that counterpublics are not necessarily virtuous or progressive, but also go further in emphasising that a multiplication of the number of counterpublics does not necessarily mean a multiplication of counterhegemonic power. For this to transpire, interconnections and solidarities between publics must occur (ibid.: 194). This echoes a much earlier assertion made by Laclau & Mouffe (1985) that only 'chains' of political activity linking through society and binding different spheres together can achieve any success with regards to the articulation of counter/hegemonic projects[24]. If this is not forthcoming, "the oppositional energy of individual groups and subcultures is more often neutralised in the marketplace of multicultural pluralism, or polarised in a reductive competition of victimisations" (Downey & Fenton 2003: 194).

Downey later continues this discussion alone (2007), suggesting two amendments to Fraser's concept of the 'subaltern counterpublic' (1992). He disagrees with the inclusion of the term 'subaltern', arguing that some counterpublics may possess relatively powerful participants, and also makes the point that the dual nature of counterpublics is not necessarily always in perfect balance. By this he means that for any given counterpublic, the balance between their inner group dynamic and their outwards-oriented public dynamic may be dysfunctional – they may be significantly better at one than the other (Downey 2007: 117). Moreover, he adds to his previous discussion (with Fenton) on the relationship between crises in the dominant public sphere and the emergence of counterpublics:

> During normal circumstances they are mostly excluded from the public sphere entirely or appear occasionally as freaks. During times of crisis and elite division, however, through skilful dramaturgical self-presentation they may penetrate the barriers of the public sphere and influence broader public opinion and may have some influence on elites and political decision-making… The extent of this depends very much, however, on the severity of crisis in the systems world, the ability of those systems to address the crisis, and the ability of elites to incorporate some of the demands of counter-publics.
>
> (Downey 1992: 118)

[24] Mouffe's continued engagement with public sphere theory will be investigated in the next section.

6.2.2.1.2 Transnationalising the public sphere

McLaughlin (1994) extends the multiple publics theme in a slightly different direction by criticising the nationalistic focus of the Habermasian public sphere. She claims that this conception of the public sphere has been outwitted by globalisation, and by evolutions in real world public spheres – formal and informal politics are increasingly transnational, and public sphere theory needs to be brought into line with these developments (McLaughlin 1994: 156). In order for this "glaring omission" to be rectified, public sphere theory must begin to engage with the "ways in which the public sphere has been reshaped through the globalising, mediated forms of communication that constitute the representational infrastructure for today's public spaces" (ibid.: 157).

Calhoun (1997) follows this lead, arguing that the Habermasian Westphalian-national public sphere ignores the "eternal reality" that citizens have always had many more societal group allegiances than just that oriented towards their nation state (1997: 89). Maintaining an insistence on the unitary public sphere, and rejecting multiple public spheres as divisive, is in fact an attempt to repress or obscure the difference that is so integral to publics, and serves only to undermine the spheres' functional capacity (ibid.: 81-82). Calhoun does, however, equally caution a blind faith in counterpublics that fails to emphasise the necessity for interpublic discourse, in that "democracy requires discourse across basic lines of difference" (ibid.: 81), and a failure to allow for this is no better than an insistence on a unitary, overarching public sphere.

Keane (2000), in his criticism of Garnham and the Westminster school's insistence on national public service broadcasting as the best contemporary realisation of the public sphere, concurs with Calhoun. "The ideal of a unified public sphere and its corresponding vision of a territorially bounded republic of citizens striving to live up to their definition of the public good are obsolete" (Keane 2000: 76). However, he goes one step further, in asserting that public sphere theory should visualise "a complex mosaic of differently sized, overlapping and interconnected public spheres" encompassing subnational through to supranational spaces and relations

(ibid.: 76). He proposes an analytical frame with which to assess real world situations by defining three levels of public spheres; micro, meso, and macro.

Micropublic spheres are defined as those existing at the subnational level, and having dozens to thousands of participants, with Habermas's coffeehouses and *salons* seen as prime examples. These may or may not emerge into the wider world of publicity and media, with this latency seen as a strength rather than a weakness.

> Although they appear to be 'private', acting at a distance from official public life, party politics and the glare of media publicity, they in fact display all the characteristics of small group public efforts, whose challenging of the existing distribution of power can be effective exactly because they operate unhindered in the unnewsworthy nooks and crannies of civil society.
>
> (Keane 2000: 78)

Mesopublic spheres have millions of participants, and exist at the nation state level, corresponding with the familiar Habermasian public sphere. They may also exist slightly within or outside the boundaries of the nation state; for example, at the regional level, or between neighbouring states who share a language or history (ibid.: 79). Macropublic spheres exist at the supranational or global level, and may have millions or even billions of participants. These categories may seem somewhat rigid, but Keane is careful to explain that they are not intended as "discrete spaces… they rather resemble a modular system of overlapping networks defined by the lack of differentiation among spheres" (ibid.: 87).

Additionally, Fraser herself has discussed this transnationalisation at length (2005). Criticising her (and others') earlier work for not going far enough towards questioning the Westphalian-national frame enclosing the Habermasian public sphere, she sets about interrogating the stability of the six Westphalian-national institutions and concepts that *Structural Transformation* is based upon: state sovereignty; economy; citizenry; language; literature; and communications infrastructure. What emerges is a picture of the comprehensive erosion of the Westphalian-national basis of the Habermasian public sphere.

> No longer unified in a single institutional locus, sovereignty is being disaggregated, broken up into several distinct functions and assigned to several distinct agencies, which function at several distinct levels, some global, some regional, some local and subnational… If public sphere communication is by definition addressed primarily to states, it cannot today serve the function of rationalising sovereign domination, as the latter is often exercised elsewhere, by non-state actors and trans-state institutions.
>
> (Fraser 2005: 4)

Similarly, the Westphalian-national economy is increasingly subsumed within globalised economic structures, typified by transnational conglomerates and financial markets. As such, an exclusively national public sphere is totally eluded by the processes that govern contemporary economic relations (ibid.). Due to migrations, disapora and dual-citizenship arrangements, there is a similar disjunct between citizenship and language, and Westphalian nation states (ibid.). The importance of national literature has also declined, partially because of increasing cultural hybridity within print media, and partially because of the increasing dominance of global visual media and entertainment. This has been facilitated by a corresponding globalisation of the communications infrastructure through privatisation, concentration and conglomeration, and new technologies such as the Internet (ibid.: 5). As such, Fraser concludes that both a horizontal and vertical multiplicity of counterpublics is necessary, rather than merely horizontal, as in Fraser (1992), in clear resonance with Keane (2000).

A cohesive public sphere theory taking all these issues into account leaves us with a vastly more flexible and plural understanding of the concept of the public sphere. It "is no longer understood as a singular deliberative space but a complex field of multiple contesting publics, including both dominant and counter-publics of various forms" (Dahlberg 2007a: 60), thus acknowledging, accounting for, and theorising the contestation of societal power differentials much more adequately than the unitary Habermasian public sphere. Furthermore, it has been de-territorialised to account for the functions and relations of an increasingly globalised and networked

world. This de-territorialisation is especially important with regards to hacktivism, given that it can be practiced on any of Keane's theorised levels, which can be seen as meshing with or complementing the various hacktivist geo-participation alignments delineated by Samuel (2003). Given the common hacktivist focus on digital rights (which are often linked in with global or at least transnational political-economic and particularly neoliberal issues and discourses) and this thesis's specific focus in on campaigns for digital freedoms, this theoretical transnationalisation is absolutely essential to the research project at hand. Furthermore, it is essential to any conception of the public sphere that wishes to comprehend the complexities and multivalent realities of our increasingly globalised society.

Continuing onwards, this improved theoretical functionality is further extended through the comprehensive discussion and critique of the public/private dichotomy at the heart of the Habermasian public sphere.

6.2.2.2 Further eroding the public/private dichotomy

6.2.2.2.1 The impossibility of bracketing status differentials and the failures of rational-critical debate

Much support has also been given to Fraser's contention that any attempts to bracket status differentials within the public sphere are counterproductive, and that an insistence upon exclusively rational-critical debate contains its own exclusionary mechanisms (Bohman 1997; Calhoun 1997; Dahlberg 2007, 2007a, 2007b; Dahlgren 1995; Downing 2001; Dryzek 2000, 2001; Eley 1992; Garnham 1992; Hoggett & Thompson 2002; Kellner 2000; Montag 2000; Mouffe 1993, 2000,

2000a, 2005; Poster 2001; Rabinovitch 2001; Ryan 1992; Squires 1998; Thompson 1993; Walzer 2002; Warner 1992, 2002).

Eley speaks of Habermas's erroneous idealisation of rational critical debate (1992: 319), and Ryan concurs, asserting that Habermas clearly did not anticipate "the fundamental critiques that feminism, in combination with postmodernism, would level against key elements in his model and his history, especially his confidence in an abstract rationality" (Ryan 1992: 262). Her history of the systemic exclusion of women from the historical public sphere not only exposes the exclusionary basis of rational-critical debate, but also identifies the need to remain open to the possibility of non-rational communication as a necessary component of public sphere theory that is truly oriented towards total inclusiveness. She argues that sometimes, political acts can be just and reasoned despite having no apparent virtue, civility, or logic, such as those carried out by the female participants in the New York Draft Riots of 1863. Her history "challenges us to listen carefully and respectfully for the voices of those who have long been banished from the formal public sphere and polite public discourse. Those most remote from public authorities and governmental institutions and least versed in their language sometimes resort to shrill tones, civil disobedience, and even violent acts in order to make themselves heard" (ibid.: 285-286). This is clearly of immense relevance to hacktivism, given its sometimes-illegal methods and often non-rational modes of discourse.

Warner (1992, 2002) continues this argument, conceptualising rational-critical publicity and the bracketing of status as a form of self-abstraction. The intention is that "the validity of what you say in public bears a negative relation to your person. What you say will carry force not because of who you are but despite who you are" (Warner 1992: 382). However, the ability to self-abstract is a differential resource, in that some are better able to do so than others; hence, "[t]he very mechanism designed to end domination is a form of domination" (ibid.: 384). Successful self-abstracters tend to be white, male, educated, propertied, and heterosexual; as such, rational-critical discourse and status bracketing compromise rather than ensure the public sphere ideal of inclusiveness. As Mouffe has also argued, "[t]o the excluded, "the 'neutral' principles of rational dialogue are certainly not so" (1993: 145).

> The bourgeois public sphere is a frame of reference in which it is supposed that all particularities have the same status as mere particularity. But the ability to establish that frame of reference is a feature of some particularities. Neither in gender nor in race nor in class nor in sexualities is it possible to treat different particulars as having merely paratactic or serial difference. Differences in such realms already come coded as the difference between the unmarked and the marked, the universalisable and the particular… the two sides of any of these differences cannot be treated as symmetrical… without simply resecuring an asymmetrical privilege. The bourgeois public sphere has been structured from the outset by a logic of abstraction that provides a privilege for unmarked identities: the male, the white, the middle class, the normal.
>
> (Warner 1992: 383)

Garnham (1992) and Thompson (1993) make the important observation that this criticism of status bracketing and rational-critical debate is not just applicable to *Structural Transformation* – it applies equally to Habermas's later theory of communicative action. "This discourse-centred concept of democracy places its faith in the political mobilisation and utilisation of the communicative force of production… it anchors the validity of norms in the possibility of a rationally founded agreement on the part of all those who might be affected, insofar as they take on *the role of participants in a rational debate"* (Habermas 1992: 447; italics in original). It is thus as equally problematic as *Structural Transformation*, leading Thompson to maintain, "it would probably be sensible for Habermas to tone down some of his stronger claims in favour of a more modest approach" (1993: 256).

Kellner (2000) also criticises this shift in thinking, in that its ahistorical and universalistic perspective does not account for the contingency, subjectivity, and constructedness of language. "Meanings and uses shift over time, while different societies have their own language games and forms of language and communication which are subject to a multiplicity of varying social forces and powers" (Kellner 2000: 11). As such, language and communication are integrally embedded in systemic power relations, and are therefore susceptible to being used for domination and manipulation. Language is, therefore, a hegemonic force, and an "imperfect model for rationality and democracy" (ibid.: 12).

Young (1996) adds another feminist voice to this line of criticism of mainstream public sphere and deliberative democracy theory. The insistence upon rational-critical arguments amongst status-bracketed individuals, while intending to secure inclusiveness, fails to acknowledge social power, and the de-equalising effect this can have on participants' confidence in their right to speak, as well as the privileging of some forms of speech over others (Young 1996: 122). As such, "[d]espite the claim of deliberative forms of orderly meetings to express pure universal reason, the norms of deliberation are culturally specific and often operate as forms of power that silence or devalue the speech of some people" (ibid.: 123). The rational-critical norms of deliberation are culturally specific and must be learned, informing a speaking style that tends to be highly correlated with social privilege. The focus on impassionate and disembodied deliberation, and literal as opposed to figurative language further reinforces this privileging of white, male, upper-class participants. Hence, those who are not socially privileged also tend not to possess the skill of rational-critical communication and are disadvantaged within deliberation. They may even 'drop out' altogether due to feelings of frustration and intimidation (ibid.: 124). Furthermore, it can be argued that passion may actually benefit reasoned deliberation aimed at understanding – a line of reasoning that would seem to inform hacktivism, particularly in its more confrontational forms:

> Reason without passion is reason without energy or dynamism. For example, if cut off from aggression, reason lacks bite and sharpness. The constructive use of aggression underpins the capacity to cut through superfluous or misleading detail and get to the heart of an issue, the ability to get hold of an argument and critically dissect it, and the ability to hold on tenaciously to a vital truth when counter-arguments are flying around.
>
> (Hoggett and Thompson 2002: 114)[25]

To counter this, Young proposes a wider understanding of the forms and styles of speech involved in political discussion, defining this revised theory as

[25] See also Walzer (2002).

'communicative' rather than 'deliberative' democracy. She proposes that the repertoire of speech acts be expanded to include greeting, rhetoric, and storytelling. Greeting is seen as a useful way in which to establish trust and respect amongst participants, and to acknowledge one another in their individual particularity. It includes expressions of leave-taking, as well as lubricating forms of speech such as mild flattery and deference which can be used to overcome any counterproductive outbreaks of hostility (ibid.: 130).

The inclusion of rhetoric is proposed in response to Young's view that "the opposition between rational discourse and rhetoric… denigrates both the situatedness of communication and its necessary link to desire" (ibid.: 131). It is not enough just to speak – one must also be listened to. Rhetoric has its place in maintaining the attention of the listener/s, as even "[t]he most elegant and truthful arguments may fail to evoke assent if they are boring" (ibid.). Finally, storytelling, or narrative, fosters understanding across difference by explaining "to outsiders what practices, places, or symbols mean to the people who hold them… Through narrative the outsiders may come to understand why the insiders value what they value and why they have the priorities that they have" (ibid.: 132-133). Hence, narrative is an important means of expressing need or entitlement, and also of contributing to social knowledge within deliberation (ibid.: 133). Young's theory of communication thus contributes to the conception of a public sphere that allows for more inclusive communication across wide cultural and socio-economic positions.

Young later embellishes her argument through an idealised, imaginary discussion between a Habermasian deliberative democrat and an activist (2001), again aiming to "sound a caution about trying to put ideals of deliberative democracy into practice in societies with structural inequalities" (Young 2001: 671). The deliberative democrat decries activism as mere interest group politics, and as having no place within the public sphere. In contrast, the activist makes the point that activism is not self-interested, it is universalist rather than partisan, and as such, cannot be reduced to an undemocratic competition between interests. Furthermore, the activist does not deny the importance of deliberation, but views activism as a necessary means of garnering attention that could not be accessed through deliberation alone. "Activities of protest, boycott, and disruption are most

appropriate for getting citizens to think seriously about that that until then they may have found normal and acceptable. Activities of deliberation, on the contrary, tend more to confer legitimacy on existing institutions and effectively silence real dissent" (ibid.: 675). As such, it is often more productive to remain outside of these institutions and protests against the socio-economic structural inequalities that condition them and participation within them (ibid.: 679).

This is obviously of massive significance to hacktivism, and, indeed, all forms of online activism. In our commercially mass-mediated societies, the privilege of being heard within the mainstream media is reserved for a privileged few. These few are, for the most part, elite sources, as has been widely explained by such theories as Herman and Chomsky's (1988) Propaganda Model, and supported by both their and screeds of other empirical research. Hacktivism seeks to overcome this elite 'attention economy', garnering attention through controversial and/or performative modes of communication and subverting the traditional hierarchies of access to public communication, by 'hacking into' the mainstream media (Vegh 2003) and thus commanding the attention of both political economic power elites and the general citizenry. They thus gain a hearing for viewpoints that would otherwise likely be ignored if they were voiced through traditional 'polite' channels and modes of communication.

Furthermore, the labeling of activists as unreasonable is exposed as a common power ploy used by societal elites to discredit activism and protest – which is certainly true in the case of hacktivism, as is evidenced by the abundance of research into its problematic conflation with the 'darker side' of hacking in general. It is argued that on the contrary, activists are generally very principled and reasoned about their causes, but have come to the conclusion that "discursive arguments alone are not likely to command attention or inspire action" (ibid.: 676). In socioeconomically stratified societies, it is antidemocratic to insist that weaker strata should 'play' strictly within the rules and forums set by societal elites who will be able to dominate the proceedings with their interests and perspectives" (ibid.: 678). The agenda, deliberative scope and constraints of such proceedings are generally dominated by hegemonic discourses (ibid.: 685-687), and as such, are better contested externally, so as to avoid the legitimation that entry confers (ibid.:

682). Furthermore, this contestation is sometimes best effected through non-discursive modes. The goal of the activist is "to make us *wonder* about what we are doing, to rupture a stream of thought, rather than to weave an argument" (ibid.: 687). As such, deliberative democracy and public sphere theory needs to understand itself primarily as "a *critical* theory, which exposes the exclusions and constraints in supposedly fair processes of actual decision making, which make the legitimacy of their conclusions suspect", and should move towards seeing the communicative sphere as far more "rowdy, disorderly, and decentred" (ibid.: 688) – a goal that this research fully supports and indeed, intends to instantiate.

Bohman (1997) reiterates Garnham (1992) and Thompson's (1993) critique of the ideal proceduralism based on rational-critical debate of Habermas's later work, and his and other deliberative democrats' erroneous assumption that these procedures will give "every citizen the equal opportunity to voice his or her reasons and to reject ones offered by others; and… ensure that dialogue is free and open and guided only by 'the force of the better argument'" (Bohman 1997: 322). In actual fact, ideal proceduralism fails to "capture the myriad ways in which deliberation may fail" (ibid.: 323) because it is guided by an inadequate conception of equality of political opportunity. Just because someone is granted formal equality does not mean that they will be accepted or treated as equal. Furthermore, rational-critical deliberation "clearly requires highly developed capacities and skills related to cognition and communications" (ibid.: 325), capacities which tend to be possessed by more socially advantaged citizens (ibid.: 325-326). That is, rational critical debate requires a form of cultural capital that is differentially allocated within stratified societies.

"Deliberative democracy should not reward those groups who are simply better situated to get what they want by public and discursive means. Its standard of political equality cannot endorse any kind of cognitive elitism"; but unfortunately, this is exactly what ideal proceduralism achieves (ibid.: 330). It results in the cumulative disadvantaging of politically impoverished or ineffective citizens. These citizens are publicly excluded, in that they cannot initiate deliberation or participate effectively in the public sphere. However, they are simultaneously politically included, since the 'common good' being discussed in the public sphere

impacts upon their existence, but "because they cannot initiate deliberation, their silence is turned into consent by the more powerful deliberators who are able to ignore them. Asymmetrical exclusion and inclusion succeed by constantly shifting considerable political burdens on the worst off, who lack the resources, capabilities and social recognition to mount a challenge to the conditions which govern institutionalised deliberation" (ibid.: 321). Rational-critical debate is once again exposed as a source of the perpetuation rather than elimination of domination and oppression – it is a legitimising force for dominant views.

Calhoun (1997) also criticises Habermas's view that private differences and status differentials are irrelevant, in line with the previous literature, as does Montag (2000), who sees the Habermasian dichotomy between reason and force as ideological. 'Reasoned' argument is constantly and irredeemably built on the foundations of "broader relationships of forces in a society characterised by a perpetual, if latent, civil war that renders some dominant and others subordinate… Behind reason, force; behind rational-critical debate the unceasing struggle of "pressure and counter-pressure"" (Montag 2000: 143-144). Hence, the Habermasian dichotomy between reason and force is ideological in that it obscures the forces constantly underpinning the differential deployment of legitimate reason.

Dryzek (2000, 2001), like Young (1996, 2001), proposes an increased tolerance to various communicative forms and practices, and differentiates himself from mainstream deliberative and public sphere theory by proposing a theory of 'discursive' democracy (Dryzek 2000: 1). He also departs somewhat from the notion of counterpublics and interpublic contestation. Instead, he conceives of an 'umbrella' public sphere enveloping a constellation of competing discourses (Dryzek 2001: 657), which is, arguably, not that far removed from counterpublic theory. In line with Young, he argues that rhetoric has a valid place within the public sphere, in that it has the ability to "reach a particular audience by framing points in a language that will move the audience in question" (Dryzek 2000: 52). Martin Luther King Jr. and the civil rights movement are given as a convincing example: "Without the emotional appeal the argument would have fallen on deaf ears. Such transmission is fully consistent with the orientation of communicative action to reciprocal understanding, so there is no need to banish it to the realm of

strategic action, as Habermas would" (ibid.). This is not to say that rhetoric does not have the possibility of coercive or manipulative use, just that it can play an important transmission function in reaching actors whose frames of reference are very different to the speakers', and who may not be at all sympathetic (ibid.: 54).

However, while agreeing in principle, he is critical of the form of Young's criticism of rational debate, in that "[t]he empirical validity of Young's claims about the degree to which these three forms of communication equalise across difference depends on the hierarchies within argument, greeting, rhetoric and storytelling compensating for, rather than reinforcing, one another" (ibid.: 67). He argues that greeting, rhetoric, and storytelling, as well as other forms of communication, are acceptable so long as they are capable of inducing reflection, do not involve coercion or the threat of coercion, and connect the particular to the general (Dryzek 2001: 660). Young's categories, as well as argumentation in general, do not necessarily satisfy these conditions (Dryzek 2000: 68).

Storytelling can be coercive if elites constrain the forms of narrative that are acceptable, and if a story is about something purely individual then there is no point hearing it. Similarly, greetings can be overly individualistic (for example, secret handshakes), and can also be coercive, such as the Maori haka. Rhetoric, as is well known, can be coercive when employed by emotional manipulators or demagogues (such as Hitler), and can become bogged down in particularism unless it actively seeks to broaden its frame of reference or span multiple frames (ibid.,: 68-70). Equally, Habermas's 'forceless force of the better argument' is only forceless if it occurs between equally communicatively capable participants. "When such equality does not hold, then in practice some individuals will be able to make their argument prevail as a result of denial of access to the premises of argument to other individuals" (ibid.: 70).

However, it is argument that Dryzek sees as central to deliberative democracy, in that it provides a means of breaching impasses that may occur with the other forms of communication, and it is a necessary component of collective action in response to social problems. Greeting, rhetoric and storytelling are all valid inclusions, but their status is slightly different in that they are not essential (ibid.: 71). Overall, "deliberative authenticity exists to the extent that communication induces reflection

on preferences in non-coercive fashion. Provided that this standard is met, the kinds of communication admissible can be quite wide-ranging, and contestation in particular should be welcomed for its ability to induce reflection" (ibid.: 76).

Dryzek also makes the important point that democratisation does not always have to be sought via the state, contrary to the assumptions made by most mainstream deliberative democrats. He criticises Habermas's newfound concentration upon elections and law making (Habermas, 1996[26]). He argues that his theory of communicative action is based upon "a naïve, civic-textbook version of democracy" (Dryzek 2000: 26), in which the state is dedicated and responsive to its citizens, ignoring the tendency for modern states to increasingly serve elite, corporate interests over its citizens (Keane 1998: 34, in McLaughlin 2004: 167). Indeed, Dryzek states that Habermas can no longer be classed a critical theorist, as he no longer believes that the state and economy (system) can be democratised any further (Dryzek 2000: 26).

He also criticises the way Habermas has "turned his back on extra-constitutional agents of both democratic influence and democratic distortion" (ibid.). Democracy "does not have to be confined to the formal institutions of state or the constitutional surface of political life. Accepting such confinement means accepting a needlessly thin conception of democracy and a needlessly tenuous account of deliberative legitimacy" (Dryzek 2001: 665-666). It is sometimes much better for counterpublics (or counter discourses, in Dryzek's theory) to remain within civil society; oriented by a relationship to the state, but not seeking any share in state power (Dryzek 2000: 93).

> If a group leaves the oppositional sphere to enter the state then dominant classes and public officials have less to fear in the way of public protest. There may be democratic gain in this entry, but there is also democratic loss in terms of a less discursively civil society, the erosion of some existing democratic accomplishments, and a reduced likelihood of further democratisation in future. Moreover, the democratic gain is itself uncertain… such gain can only be secured when the defining

[26] "Informal public opinion-formation generates "influence; influence is transformed into "communicative power" through the channels of political elections; and communicative power is again transformed into "administrative power" through legislation." (Habermas 1996: 28)

> interest of the entering group can be connected quite directly to an existing or emerging state imperative.
>
> (Dryzek 2000: 80-81)

Political power can be exerted within civil society in numerous ways, especially because it is a far less constrained space than the state (ibid.: 96). It can affect the way terms are defined and issues are framed within political discourse, rather than through the "direct leverage of one actor over another. The relative weight of competing discourses in civil society can have major implications for the content of public policy" (ibid.: 94). Social movements can permanently alter political culture by legitimating certain forms of protest action, and through the introduction of issues into the public agenda. Policy-oriented deliberative arenas can be established within civil society, and "protest within civil society can create fear of political instability and so draw forth a governmental response" (ibid.). Furthermore, civil society actions can generate cultural change, with repercussions for wider power relations.

These points highlight the strengths of hacktivism as a form of political communication, with the importance and validity of maintaining a vibrant public sphere existing in separation and opposition to the state once again underlined. While much hacktivism is indeed somewhat oriented towards one or more nation states, it is just as likely to be oriented towards 'elite, corporate interests' (often in combination with a state focus), thus comprehending and opposing the increasingly close-knit elite political-economic alliances present within global modernity. In such an environment, focusing entirely upon state structures, let alone seeking to capture some modicum of state power, is a misguided (and extremely difficult) objective – indeed, as Dryzek argues, hacktivists retain much more agility and counterhegemonic power by remaining firmly outside the institutional political system. They retain the freedom to both introduce new issues into the public arena and frame them in their own terms, and can also incite enough public unrest that a governmental response is forced. Hacktivism is also arguably being established as an increasingly recognised (if not entirely condoned) form of activism, with recent actions undertaken by the group Anonymous more and more often described by

multiple news sources as 'activism' (as opposed to cyberterrorism or hacking) and with the word 'hacktivism' gradually entering the vocabulary of mainstream media outlets such as the BBC ('Anonymous hacktivists say Wikileaks war to continue' 2010).

Dahlberg is the most recent addition to the multitude of voices critiquing the impossibility of effectively bracketing status differentials within the public sphere or spheres of debate, as well as the Habermasian insistence on rational-criticality. Originally what might be described a 'staunch Habermasian'[27] (2004, 2005), he accepted the discussed field of public sphere theory as highlighting some important issues, but as constructing its criticisms of Habermas on an under-sophisticated reading of his works, particular his later theory of communicative rationality. He does raise some valuable issues in these earlier works, which are based on an extremely sensitive and deep reading of Habermas, although his counter-criticisms of the criticisms made by what he classes 'difference democracy theory', are, at times, arguably based on forced theoretical contortions in defense of Habermas.

However, Dahlberg now considers mainstream or Habermasian public sphere theory, while "pay[ing] more attention to power than some critics argue", as failing to "adequately theorise the power relations involved in defining what counts as legitimate deliberation" (Dahlberg 2007: 47), and his recent works emerge from what he calls 'agonistic' public sphere theory (2007, 2007a, 2007b). He has become fully engaged in the project of radicalising the public sphere concept. However, this does not mean that he has totally abandoned mainstream public sphere theory as useless; rather, he argues that it has not gone far enough. While it conceives of power deriving from coercive action, instrumental or strategic action, technical limitations and social inequalities, it does not *adequately* acknowledge the disciplining and negative power it enforces through legitimising only rational-critical deliberation, and the way in which this privileges those whose native modes of communication (generally Western, masculine modes) are closer to this ideal (Dahlberg 2007: 131, 2007a: 53).

[27] In the sense that he subscribed strongly to Habermas's later theory of communicative action or rationality.

While sophisticated mainstream deliberative democrats do acknowledge this phenomenon, they see it as resulting from 'cultural bias'; it is simply another kind of 'distorted communication' that advantages some participants due to their cultural context instilling them with more 'legitimate' voices (Dahlberg 2007: 131). Furthermore, they see the idealised public sphere norm (or, indeed, any idealised norm) as fallible and open to reinterpretation. Hence, any application of this norm will likely have anti-democratic effects in the form of exclusions. Nonetheless, they do believe that the perfection of the normative conception of and realisation of the ideal form of the public sphere is theoretically possible.

In contrast, this is where poststructuralist critics disagree. They see meaning as inherently unfixed and therefore all rational communication as, necessarily, a failure. While this difference in belief does not translate into an understanding of power and exclusion within the public sphere that is any different from mainstream theory (in that both assume that the ideal public sphere is never realised), it makes a huge difference with regard to how the inevitable exclusions from the public sphere are dealt with:

> The deliberative democrat focuses upon how to achieve more rational critical debate within communicative spaces, while their feminist/poststructuralist critics focus on the power and exclusion involved in the institution of such communication… By ignoring this politics, the deliberative position fails as a radically democratic norm, which must account for how all voices can participate in political processes.
>
> (Dahlberg 2007: 132)

This is why mainstream deliberative or public sphere theory has no place for "non-deliberative activist protest actions. Such actions are not recognised in the deliberative model's emphasis on reciprocal, respectful communication" (Dahlberg 2007: 133). However, as Dahlberg argues, agonistic public sphere theory (to use his term) expands the repertoire of legitimate modes of communication to

potentially allow this kind of action (given that it meets certain basic criteria, as Dryzek has made clear), primarily through the deployment of the counterpublic concept. It does not deny the central role of deliberation; it simply adds the idea of discursive contestation to the emphasis on deliberative politics. Rather than simply accepting rational-critical deliberation as the only legitimate form of discourse, neo-Habermasian public sphere theory allows for both discursive radicalism and interdiscursive contestation.

Drawing on poststructuralism and a post-Marxist understanding of discourses as "socially contingent systems of meaning, which form the identities of subjects and objects", each discourse is seen as fundamentally predicated upon exclusion (Dahlberg 2007b: 835). "There is always an 'outside' to discourse, a set of meanings, practices, identities and social relations, which is defined by exclusion and against which discursive boundaries are drawn" (ibid.). Discourses are therefore fundamentally political, in that they are involved in constant hegemonic struggles over the limits of everything, including what can be counted as 'legitimate' deliberation (ibid.). As such, discursive radicalism is that against which the norm of rational-critical debate is defined – the 'radical other'. This struggle between the 'normal' and the 'radical' is constant, preventing discursive or hegemonic closure of the boundaries of legitimate public sphere deliberation. Counterpublics are the space in which radical discourses are practised and solidified; made ready for interpublic or interdiscursive contestation with other counterpublics and the dominant public sphere (Dahlberg 2007a: 54-55):

> The agonistic public sphere understanding, through the key concept of counter-publics, makes central both intra-discursive deliberation that constitutes publics (as against interest groups) and inter-discursive contest that challenges deliberative exclusions. The result is a radicalised public sphere conception, radicalised in relation to the deliberative model in that it extends public sphere theory to include politics associated with voices excluded from mainstream public spheres. The radicalised conception gives democratic legitimacy to voices and struggles from outside what is deemed within any particular political context to be 'legitimate' deliberation.
>
> (Dahlberg 2007: 140-141)

As such:

> …protest is very much a communicative act when undertaken with the aim of raising issues for deliberation rather than to coerce. The use of signs and banners, street demonstration, guerrilla theatre, dance and song, offline and online sit-ins, cyber-parody, graffiti and posters, etc. utilise creative and sometimes 'disruptive' forms of rhetoric through which marginalised groups can gain a hearing for their voices and call into question more dominant positions.
>
> (Dahlberg 2005: 119-120).

This argument aligns with Young's previously discussed call for the inclusion of activism and other more 'rowdy' and passionate forms of communication within the public sphere (1996, 2001), and is similarly essential to an understanding of the public sphere that can help us explore hacktivism's role in modern democracies. Hacktivism most certainly aims to raise issues for deliberation through creative, performative and often disruptive forms of direct online protest, thus garnering attention for marginalised or counterhegemonic discourses and opinions, and calling positions of dominance or hegemony into question.

Overall, Dahlberg rounds off a convincing critical body of theory based on the futility and counter-productivity of Habermasian public sphere theory's insistence upon the bracketing of status within the public sphere, and its similarly erroneous focus on exclusively rational-critical deliberation at the expense of forms of contestation. However, there is a final subsection of criticism that must be addressed before we can provide a full understanding and thus concise explanation of neo-Habermasian theory.

6.2.2.2.2 Democratic advantages in allowing private interests into the public sphere, and the failure of consensus

Neo-Habermasian theory also follows Fraser's (1992) lead in problematising Habermas's strict demarcation between public and private and his insistence that private issues have no place within the public sphere, as well as her questioning of the possibility and legitimacy of consensus (Benhabib 1996a; Calhoun 1994, 1997; Daniel 2000; Dahlberg 2005, 2007, 2007a, 2007b; Dryzek, 2000, 2001; Felski 1989; Gould 1996; Lyotard 1984; Mouffe 1993, 1996, 2000, 2000a, 2005; Sassi 2000; Ryan, 1992; Warner, 1992). Through allowing for contestation as well as deliberation within public sphere theory, we have already implicitly questioned the need for all public sphere communication to be oriented towards consensus. Similarly, through exposing the impossibility of bracketing status differentials, we have also problematised the notion that the private world should be kept totally separate from the public sphere. We will now investigate both of these issues in more explicit detail.

6.2.2.2.2.1 Allowing private interests into the public sphere

Ryan (1992) once again proves a starting point, with her discussion of the history of the emergence of American female public spheres illustrating that "the notions of interest and identity need not be antithetical to the public good… In practice, inclusive representation, open confrontation, and full articulation of social and historical differences are as essential to the public as is a standard of rational and disinterested discourse" (Ryan 1992: 285). Indeed, women only gained emancipation and entry into the mainstream public sphere through articulating their personal interests and desires through counterpublics, arguing towards equality and admittance into the mainstream. The same could be said for the argument for

universal and unrestricted internet access – over the last few decades, it has moved from something viewed predominantly as a private concern, towards a right that is increasingly ratified by national legislation and vigorously defended as a public good when threatened.

Warner (1992, 2002) concurs with the importance of facilitating the ability to introduce 'private' interests into the public sphere, and generalises this issue outwards to include multiple fields of private differentiation: "Neither in gender nor in race nor in class nor in sexualities is it possible to treat different particulars as having merely paratactic or serial difference" (Warner 1992: 383). These private issues and interests require introduction rather than elimination within the public sphere if it is to be a truly egalitarian discursive arena or network of arenas. "To make the distinction between private and public is to determine the subjects of common discussion and decision and thus the borders of politics" (Sassi 2000: 95), when a truly democratic public sphere theory requires that these borders be kept open to contestation. "Democratic publicity requires positive guarantees of opportunities for minorities to convince others that what was not public in the past should be so now" (ibid.: 93). As such, counterpublics need not only be formally political, but may be based around cultural and identity issues as well (Warner 2002; Schiller 2007).

Calhoun agrees, arguing that Habermas's perception of the degradation of the public sphere in *Structural Transformation* is partially based upon a failure to acknowledge that the public sphere concept has dual functionality – it is oriented not only towards 'problem-solving' but also towards 'world-disclosing' (ibid.; see also Calhoun 1997:82). The problem solving function of the public sphere has arguably degenerated somewhat, but it is difficult to make the same argument about its world-disclosing function, in that public discourse has not become a "less vibrant source of understanding, including self-understanding"(Calhoun 1994: 34).

Furthermore, this world-disclosing role is not limited to political culture, as many cultural and identity-based issues are increasingly and fundamentally linked to political struggles. As Benhabib notes, there has been widespread shift away from formal-governmental politics and strictly socio-economic preoccupations, towards a politics increasingly oriented around identity and difference (Benhabib, 1996a: 4).

This movement gives us a reason to be less despairing in the face of increasing disengagement from and disillusionment with formal politics (Blumler & Gurevitch 1995; Eliasoph 1998; Putnam 2000; Sandel 1996). When we look at these 'new' politics, "we can see various signs that suggest that many people have not abandoned engagement with the political, but have rather refocused their political attention outside the parliamentary system", with politics becoming "not only an instrumental activity for achieving concrete goals, but also an expressive activity" (Dahlgren 2007: 57).

These identity-based politics, primarily in the form of the so-called 'new social movements'[28], have come under some criticism, with Gitlin (1995) claiming that they are a weak substitute for 'real world' politics based upon economic inequalities. He argues that identity-politics are destructive in that they fragment the 'left', ignore core issues of economic inequality, and provide no means for broad unification against the dominant capitalist powers; thus, bringing democracy to a new crisis. However, as Giroux asserts, this criticism is characteristic of a totalizing view of class that cannot conceive of culture and class as being intertwined (2000: 257). It sees social class as static, as opposed to dynamic and negotiated, and ignores the historical use of class politics to demean issues of gender, race and sexual orientation (ibid.: 254). Class is actually lived through modes of race and gender; hence, the new social movements are part of a class-based politics, not external to it (ibid.). "Social group designation and experience is meaningful for the expectations we have of one another, the assumptions we make about one another, and the status we assign to ourselves and others. These social group designations have serious consequences for people's relative privilege or disadvantage" (Young 1997: 386).

When Habermas "treats identities and interests as settled within the private world and then brought fully formed into the public sphere, he impoverishes his own theory", just as he does when assuming that these interests and statuses can be bracketed (Calhoun 1994: 35). Social movements (of all kinds) are seen as having a

[28] Movements arising from the Sixties onwards, such as environmentalism, women's rights, and sexuality-based movements. These movements are seen as 'new' in that they are not explicitly or exclusively class-based. They do not limit themselves to seeking material gain, but challenge the very notions of politics and society (Della Porta & Diani 2006: 8-9). See also Melucci (1982, 1989, 1996).

strong role in relation to this, in that they are important for restructuring identities as well as issues. They are also "crucial to reorienting the agenda of public discourse, [and] bringing new issues to the fore. The routine rational-critical discourse of the public-sphere cannot be about everything all at once. Some structuring of attention, imposed by dominant ideology, hegemonic powers, or social movements, must always exist. The last possibility is crucial to democracy" (ibid.: 37). Hacktivism in support of digital rights (or indeed any cause) is clearly intended to effect this 'structuring of attention', bringing their chosen issues to the notice and consideration of elites and the citizenry at large through performative publicity-generation.

And indeed, Habermas's later theory of communicative action does see new social movements as an integral part of the public sphere, arising in response to the systemic colonization of the lifeworld. This colonization has disturbed traditional forms of life, thus catalyzing the questioning of many previously unquestioned aspects of society. This questioning has occurred in a political context, in that systemic intrusions into the lifeworld serve to politicize it; thus, every day life has become politicized (Roberts & Crossley 2004: 9). "[N]ew social movements form new, critical publics. By means of communicatively rational engagement they call the system into question and set the agenda for a normative revitalisation of it" (ibid.). However, he still does not acknowledge that actions within the public sphere may actually be constitutive rather than merely reflective of private identity, which is a mistake, as "in varying degrees all public discourses are occasions for identity-formation" (Calhoun 1997: 86).

6.2.2.2.2.2 The impossibility of consensus

Thompson (1993) initiates further criticism of Habermas's orientation towards consensus through rational-critical debate, arguing that in a contemporary pluralist democracy, the emergence of a legitimate consensus is unlikely. However, it is Chantal Mouffe who makes the largest contribution towards critiquing the

possibility of eradicating disagreement within the public sphere. Drawing on her post-Marxist[29] work with Ernesto Laclau (1985), she has reiterated her theory of agonistic pluralism in multiple pieces of literature (Mouffe 1993, 1996, 2000, 2000a, 2005). Mouffe summarises that, for Habermasian public sphere theory, "the process of deliberation is guaranteed to have reasonable outcomes to the extent that it realises the condition of the "ideal discourse": the more equal and impartial, the more open the process is, and the less the participants are coerced and ready to be guided by the force of the better argument, the higher the likelihood that truly generalisable interests will be accepted by all those relevantly affected" (Mouffe 2000a: 5-6). However, the Habermasian belief that obstacles to reaching this legitimate rational consensus are empirical; that is, that due to the constraints of social life it is unlikely that citizens will ever be able to transcend personal interests enough to attain true universal rationality; is erroneous (ibid.: 6).

In actual fact, the obstacles to rational consensus are ontological (Mouffe 2000a: 13). A "nonexclusive public sphere of rational argument where a non-coercive consensus could be attained" is an impossibility (Mouffe 1996: 255), because the presence of difference, seen as an impediment to be overcome, is the very thing that makes deliberation possible and necessary (Mouffe 2000a: 13). Difference is actually the key to deliberation. If a true consensus were ever reached, the need for deliberation and thus the deliberative public sphere would instantly disappear:

> …the belief that a final resolution of conflicts is eventually possible, even if envisaged as an asymptotic approach to the regulative ideal of a free and unconstrained communication, as in Habermas, far from providing the necessary horizon of the democratic project, is something that puts it at risk… [P]luralist democracy contains a paradox, since the very moment of its realisation would see its disintegration. It should be conceived as a good that only exists as good so long as it cannot be reached.
>
> (Mouffe 1993: 8)

[29] Post-Marxism links in with 'new' identity-based politics, in that it turns away from the strict Marxist focus on class, towards a more complex understanding of political identity (Dyer-Witherford 2007: 193). However, in addition, socio-political identities are conceived in a poststructuralist or postmodern sense as being unfixed. Instead, they are constantly redefined in a fashion relative to all other identities. Political movements arise due to antagonisms between different signifiers that define themselves against one another.

As such, "pluralism is not merely a *fact,* something that we must bear grudgingly or try to reduce, but an axiological principle. It is taken to be constitutive *at the conceptual level* of the very nature of modern democracy and considered as something that we should celebrate and enhance" (Mouffe 2000: 19).

Furthermore, power can never be eliminated from social relations, due to the fact that all social objectivities or identities are based upon acts of exclusion, and will always bear traces of this constitutive exclusion. In other words, as was already argued by Dahlberg, identities are premised upon a we/they dichotomy, so each and every 'we' contains traces of the 'they' it is defined against (Mouffe 1993: 2-3). Power is therefore an ineradicable and intrinsic component to any identity, rather than an externality. In addition, this 'we/they' relationship always contains the possibility of degradation into an antagonistic friend/enemy dichotomy. Antagonism, then, can never be eliminated, and constitutes an ever-present possibility within politics (Mouffe 2000: 12).

As such, Mouffe argues for a democratic model that places issues of power and antagonism at its very centre, designating it a model of 'agonistic pluralism' (2000: 97). This model sees the main task of democratic politics as not to attempt to eliminate power and antagonism, as this is impossible, but to try and defuse it and constitute it in more democratic terms. Enemies must be transformed into adversaries, and antagonism into agonism (Mouffe 2000a: 16). An adversary is defined as "somebody whose ideas we combat but whose right to defend those ideas we do not put into question" (ibid.: 15). We acknowledge them as a legitimate opponent in that they share an orientation towards the democratic principles of liberty and equality; however, we both conceive of these terms differently in terms of meaning and implementation, and as such, we are unable to resolve our disagreement via rational deliberation. Hacktivism is arguably an example of Mouffe's call for the transformation of antagonism into agonism – it avoids violence, but retains passion, and vigorously contests the ideas of opponents without ever seeking to annihilate them or permanently deny them the right of response.

This conception of agonistic plurality sees no possibility of a rational consensus, as we are engaged in "a struggle between opposing hegemonic projects which can never be reconciled rationally" (Mouffe 2005: 21). An agreement can only be

found if one or both of us undergoes a "radical change of political identity" (Mouffe 2000a: 15), given that "the very condition for the creation of consensus is the elimination of pluralism from the public sphere." (2000: 49). However, this is not to deny the fact that alliances between subordinate groups - 'chains of equivalence' based on their equally subordinate status - must be constructed in opposition to that which subordinated them (Laclau & Mouffe 1985; Mouffe 2005: 53). A failure to do this actually obscures the recognition of certain differences as relations of subordination (Mouffe 1996: 247).

Young has taken a similar stance regarding the Habermasian orientation towards consensus (1996, 1997), in that it assumes that the participants in deliberation either "begin with shared understandings or take a common good as their goal" (Young 1996: 120). There are a number of problems with both of these assumptions. Firstly, it cannot be assumed that "there are sufficient shared understandings to appeal to in many situations of conflict and solving collective problems" (ibid.: 125). Secondly, and in line with Mouffe, Young argues that the assumption of a prior unity that merely requires rediscovering obliterates the need for deliberation in the first place. Some Habermasian deliberative democrats respond to this second criticism by theorising unity (or consensus) as a goal to be worked towards, rather than something to be rediscovered. The problem here harks back to the failures of rational-critical debate. The theoretical consensus is oriented towards the 'common good', but as we have discussed, some groups (generally societal elites) are better positioned to control the definition of this 'common good' than others; thus, the status quo is reified (ibid.: 126).

Rather than orienting debate purely towards consensus, Young argues that it should focus on attaining a minimum level of unity, and that engaging in deliberation with a spirit of openness and accountability is sufficient (Young 1997: 402). Differences should be viewed as resources, rather than something to be transcended. In recognising that the others we are encountering are different - "[t]his does not mean that we believe we have no similarities; difference is not total otherness" - then we also recognise that there is something to be learned from them "precisely because the perspectives are beyond one another and not reducible to a common good"

(ibid.: 127). In this way, the plurality that is a necessary condition of publicity (again, in line with Mouffe) is maintained.

> A conception of publicity that requires its members to put aside their differences in order to uncover their common good destroys the very meaning of publicity because it aims to turn the many into one.
>
> (Young 1997: 401)

Rather than a falsely rational consensus, the end result of Young's communicative democracy theory is a level of understanding based upon the self-transcendence privileged by deliberative democrats. Personal perspectives are exposed as just that; the knowledge that one is arguing with diverse others requires one to frame arguments in ways that best bridge these differences in order to have any chance of success; and the expression and questioning of difference generates a greater social knowledge or subjectivity that increases participants' "wisdom for arriving at just solutions to collective problems" (ibid.: 129). She acknowledges that this is, indeed, an ideal, but argues that it can serve three important functions:

> …to justify a principle of the inclusion of specific group perspectives in discussion; to serve as a standard against which the inclusiveness of actual public communication can be measured; and to motivate action to bring real politics more in line with the ideal.
>
> (Young 1997: 404)

Dryzek (2000, 2001) is also critical of the Habermasian focus on rational-critical deliberation in which "consensus remains the regulative ideal, an orientation to which real-world arrangements could aspire, though never actually reach" (Dryzek 2000: 48). In line with Mouffe and Young, he also argues that the attainment of consensus would eliminate all the difference or plurality that makes deliberation possible and necessary (Dryzek 2001: 661). He believes that a focus on public

reason can be maintained despite this reason being plural, and 'workable agreements' generated.

> Workable agreements that can secure assent for different reasons are more plausible. Discursive legitimacy is achieved to the extent of the resonance of such an agreement with the prevailing constellation of discourses in the degree to which this constellation is subject to dispersed and competent control.
>
> (Dryzek 2001: 665)

Dahlberg (2005, 2007b) agrees with the characterisation of the emergence of any real-world 'consensus' as merely the hegemonic stabilisation of meaning made possible through domination or exclusion. Discursive contestation is essential for questioning this consensus or hegemony, with consensus representing "simply one point in a dynamic process" (Dahlberg 2007b: 836) – no true, final consensus can ever be reached. The means are infinitely more important than the end; that is; the process of deliberation and contestation is infinitely more democratically valuable than any of the temporary and flawed 'consensual conclusions' to this process (Dahlberg 2005: 127-128).

6.3 The neo-Habermasian public sphere: A new normative ideal

It should by this stage be abundantly clear that there is a broad support base for a reworking of Habermasian public sphere and deliberative democracy theory in a way that allows for a more adequate acknowledgement and contestation of societal power differentials. We will call this reformulation 'neo-Habermasian public sphere theory', in that it retains the Habermasian public sphere as its departure point or core, but expands and sensitises it in new ways, thus more effectively

comprehending issues of power and difference. In the words of Ryan, it allows publicness to "navigate through wider and wilder territory" (1992: 286).

Neo-Habermasian public sphere theory is defined by the following:

1. The theorisation of multiple public spheres:
    a. These spheres and the discourses constituting them are defined against or in opposition with one another, and with the dominant public sphere or spheres. As such, they are known as 'counterpublic spheres'.
    b. These spheres may range in size/scope from sub-national to supra-national.
    c. They are public in that they have an outwards orientation – they aim to engage with other public spheres – as well as an inwards, group-solidarity-based orientation.
    d. Because demarcating an *a priori* boundary around what issues may be included within the public spheres is exclusive, and status-bracketing is impossible, counterpublics may be based around a range of concerns, and these concerns may be fully articulated within the public spheres. In effect, everything can be political if it is determined as such through deliberation.

2. The realisation that exclusively privileging rational-critical debate as the only mode of legitimate communicative action within the public sphere is exclusionary:
    a. As such, multiple modes of communication are deemed legitimate, including contestation and diverse forms of deliberation.
    b. However, these diverse modes of communication should still be judged in accordance with how well they fulfill a normative ideal of deliberative legitimacy. This 'deliberative authenticity' exists to the extent that communication induces reflection on preferences in a non-coercive fashion (Dryzek, 2000, 2001).

c. Achieving truly rational consensus is impossible in that it eliminates plurality, and any 'consensus' actually attained will always based upon exclusion and hegemonic stabilisation. 'Workable agreements' or temporary consensus will suffice, but should always remain open to contestation. The processes of deliberation and contestation are what have true value.
d. Communicative action does not necessarily need to be oriented towards the state – it can have powerful effects within civil society.

This updated theory of the public sphere (or spheres, to be more precise) is far more realistic, useful, and flexible that its original incarnation within *Structural Transformation*. Rather than presenting a contradictory, dated, and unattainable ideal, it provides us with the tools needed to investigate the contemporary world and particularly the contemporary mediated landscape of political communication, and of effectively comprehending and hopefully contesting the lines of power running through the societies in which we live. We now have a theoretical lens through which we can investigate the phenomenon of hacktivism.

The final three chapters interpret three cases of hacktivism through a neo-Habermasian theoretical lens. Rather than being randomly selected, these case studies focus in on a particular subject of contention – the ongoing and intensifying struggle over the development and control of the Internet. Hacktivist incidents from each category of Samuel's typology – political coding, performative hacktivism, and political cracking – are subjected to a critical discourse analysis guided by the concerns of neo-Habermasian public sphere theory. This analysis focuses on both the forms of the hacktivism, and on the texts produced by it. This attention to both discursive form and discursive content is structured by a focus on issues of diverse access to speech and attention and thus communicative power. However, let us first pull together the two threads of neo-Habermasian public sphere theory and hacktivism, thus establishing that hacktivism is indeed a legitimate form of neo-Habermasian public sphere communication and solidifying the foundation upon which the following analytical chapters rest.

6.4 Hacktivism: A legitimate form of neo-Habermasian public sphere communicative activity

As has been explored within this chapter, as long as activism (including hacktivism, or indeed, any form of communicative activity) fulfills the requirement of inducing preference-reflection in a non-coercive fashion, it is an entirely legitimate mode of participation within the neo-Habermasian public sphere. The goal of the activist is "to make us *wonder* about what we are doing, to rupture a stream of thought, rather than to weave an argument" (Young 2001: 687). 'Repertoires of electronic contention' utilizing 'conventional' and 'disruptive' tactics (Costanza-Chock 2001) can be understood as constituting different modes of internet-based counterpublic spheres, which are then further defined by the discursive struggles they elect to take part in, and the discourses they articulate.

These mobilisation outcomes or modes of activism range from tactical Internet use focused on information creation and diffusion, and the organisation and co-ordination of 'street' mobilisations (conventional mobilisation and cultural outcomes), to collective or individual action using the Internet itself as a platform for activism. This latter 'disruptive' category encompasses various tactics or 'cultural outcomes', such as site redirection/alteration/imitation, various floods (such as email or form), client or server-side denial-of-service attacks, and the use of trojans or viruses, and political software development; that is, different forms of hacktivism. Unless these conventional and disruptive tactics morph into violence proper, and/or are used by governments or militaries (thus becoming cyberterrorism or cyberwarfare), they would seem to fulfil the neo-Habermasian public sphere requirement of being intended to provoke non-coercive reflection on any preferences or opinions one might have formed regarding a given issue.

As such, hacktivism would appear to fulfil the neo-Habermasian requirement of provoking reflection on political preferences in a non-coercive manner, and it most certainly intends to destabilise the dominance or hegemony of more powerful discourses or publics. It is temporarily disruptive, but it does not result in human,

infrastructural or serious financial casualties, it does not violently force or coerce preference alteration, and it does not seek to annihilate enemies, but rather to dispute adversarial discourses. Indeed, this is true for all non-violent activism and protest, both online and offline. As Dahlberg has contended:

> [P]rotest is very much a communicative act when undertaken with the aim of raising issues for deliberation rather than to coerce. The use of signs and banners, street demonstration, guerrilla theatre, dance and song, offline and online sit-ins, cyber-parody, graffiti and posters, etc. utilise creative and sometimes 'disruptive" forms of rhetoric through which marginalised groups can gain a hearing for their voices and call into question more dominant positions.
>
> (Dahlberg 2005: 119-120)

Hacktivism therefore merits analysis as a counterpublic activity, constituted as it is by counterhegemonic discourses oriented towards the contestation and destabilisation of targeted dominant or hegemonic publics. We should seek an improved understanding of how these counter-discourses are propelled into wider consideration using online iterations of traditional protest activities. Allowing contestatory forms of non-coercive communication into the public sphere, rather than requiring all participation to fulfil rational-critical criteria, goes some way towards counteracting or at least challenging the differentials of communicative and political power present in the tremendously stratified societies within which we exist, and is thus an important objective. It is telling that the Kiwicon attendee who indicated that he had been involved in hacktivism defined it in a manner that signalled his implicit agreement with this theoretical perspective:

> [Hacktivism is] exercising an implied right towards political discussion through circumvention of electronic mediums. […] [It provides an] equal medium in order to express yourself.
>
> (Farrell 2007a)

As such, the remainder of this thesis will explore how hacktivism functions as a for of online counterpublicity intended to provoke political preference reflection, and destabilise dominant publics and thus threaten hegemony, through a critical discourse analysis of the three previously outlined, theoretically sampled case studies. That is, the analysis will address the second research question:

> *How does hacktivism, through discursively constructed and externally oriented publicity, function as a counterpublic sphere or counterhegemonic project oriented towards the provocation of political preference reflection and the destabilisation of a given dominant or hegemonic public?*

Each case study interprets an instance of hacktivist activity through a neo-Habermasian lens, investigating the way in which they provoke political preference reflection in aid of the destabilisation of a given dominant or hegemonic public. The following chapter examinees the political coding group, Hacktivismo, with the subsequent two chapters then focusing on the New Zealand-based performative hacktivism of the Creative Freedom Foundation, and the political cracking carried out by a subsection of the group known as Anonymous.

Chapter 7

Political coding: The case of Hacktivismo

7.1 Context

Hacktivismo is a hacktivist group that emerged as an offshoot project of the prominent Texas-based hacker group and DIY media organisation, the Cult of the Dead Cow (cDc).[30] The cDc have a reputation as "the elite of the hacker world" (Samuel 2004a: 88), and are also one of the oldest groups of hackers. The then-14 year old hacker, Grandmaster Ratte'[31], co-founded the cDc with Franken Gibe and Sid Vicious in Lubbock, Texas, in 1984, and their name stems from their original group space – an abandoned slaughterhouse in their meat-packing home town, which served as a hangout for Lubbock youths in general (Einhorn 2002). They were one of the first groups to attach a specific political agenda to hacking, and also recognised the role of the media in helping them disseminate this agenda – as such, they have been much more visible (through media appearances) than many other hacker groups.

Prior to the emergence of Hacktivismo, the cDc gained notoriety for developing Back Orifice, a programme that exploits (with the intent to draw attention to) some major security holes in versions of the Windows OS to allow remote network administration. The initial version worked with Windows 95 and 98, and a more recent version, Back Orifice 2000 (B02k), supports Windows XP and 2000. They are also known for their 'Goolag' campaign, which criticised Google's decision to censor its Google.cn searches (under the direction of the Chinese government) in order to gain entry into the Chinese market), as well as similar compliance by

[30] Much of the information in this section comes from the Cult of the Dead Cow Communications' and Hacktivismo's main websites – www.cultdeadcow.com and www.hacktivismo.com - and will not be referenced directly, as it would generate too many inline citations. However, direct quotes and material from other sources will be referenced as normal. Furthermore, cDc rather than CDC is the Cult of the Dead Cow's preferred acronymic style, and is therefore what shall be used.

[31] Almost all Hacktivismo members, in line with political coders in general, use pseudonyms or handles rather than their real names.

Microsoft, Yahoo! and Cisco (see Figure 4). (It is worth noting that Google have now pulled out of China, through diverting all Google.cn requests to the uncensored Google.hk domain.)

Figure 5: The cDc's Goolag campaign logo[32]

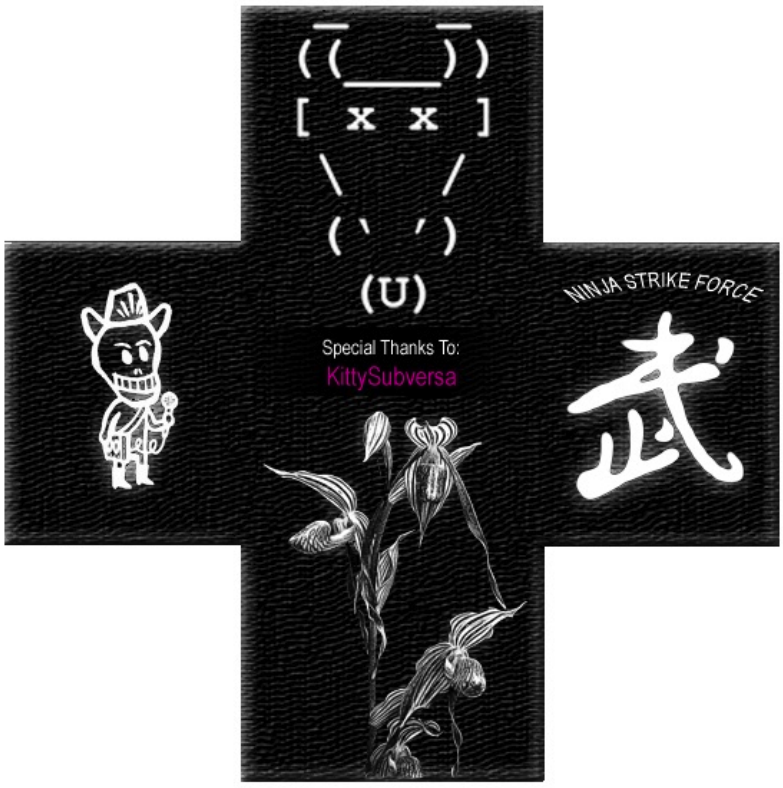

Figure 6: An 'easter egg' (surprise content) within Torpark, one of Hacktivismo's projects, showing (left, top, right) Hacktivismo, cDc and Ninja Strike Force imagery[33]

[32] Image from: http://w3.cultdeadcow.com/cms/2006/02/cdc-launches-gl.html
[33] Image from: http://en.wikipedia.org/wiki/File:Torpark_DEADBEEF_eegg.gif

The cDc also function as an alternative media outlet, producing their own books, online texts, music, and videos. They are one of what is now a triumvirate of cDc entities, the other two being the Ninja Strike Force and Hacktivismo. Formed in 1996, the Ninja Strike Force is a group of specially selected, elite cDc hackers who are dedicated to achieving the various offline and online goals of the cDc. Hacktivismo, who are the focus of this case study, were formed in 1999. These three groups together constitute cDc Communications (see Figure 5).

7.1.1 The emergence of Hacktivismo

Hacktivismo describe themselves as an international 'special operations group' and were founded by the cDc's 'Foreign Affairs Minister', Oxblood Ruffin, and sponsored by the cDc. They "view access to information as a basic human right" and are "also interested in keeping the Internet free of state-sponsored censorship and corporate chicanery so all opinions can be heard" ('The Hacktivismo FAQ v1.0'). They state that they are "trying to intervene to reverse the tide of state-sponsored censorship of the Internet through the inventive use of code… [and] favour using disruptive technologies that comply with the spirit and original intent of the Internet" ('The Hacktivismo FAQ v1.0'). As of July 2001, they had five core official members – Ruffin, Bronc Buster, The Pull, Mixter, and Drunken Master (a.k.a. Paul Baranowski), as well as a wide cohort of contributors from all over the world:

> Our numbers include I.T. professionals, lawyers, human rights workers, and students. We live in the United States, Canada, Europe, Israel, Taiwan, Korea, and the Peoples Republic of China. Hacktivismo also has informal layers of support that collect network intelligence and will assist with application distribution, and document translation. The one thing that can be said of the Hacktivismo network is that it is truly

> international. We're the United Nations of hacking, except without the bickering and cheapskates who won't pay up.
>
> ('The Hacktivismo FAQ v1.0')

Ruffin will only extend membership invitations to individuals once they have invested a lot of time in Hacktivismo projects, keeping the core membership reserved for a dedicated elite. Ruffin has a PR background, having worked for the United Nations for 10 years, and is (relative to the other hackers in the cDc) "not in the least technical" (Ruffin, 2002, in Samuel 2004a: 90). He was invited to join the cDc in 1996 (again, membership is by invitation only) after making contact with one of their members, Death Veggie. Ruffin is described as the one who took the term and concept of hacktivism and ran with it (although it was reportedly first coined by cDc member Omega, who initially used it jokingly to describe on-line protest actions). Ruffin, however:

> …appropriated the word and began using it with a straight face; then many journalists, fading stars of the Left, and eventually script kiddies picked up on it, all claiming to know what hacktivism meant. It has been a noun in search of a verb for some time now. Oxblood once defined hacktivism as "an open-source implosion", and now he's added "disruptive compliance" to its range of description… [that is,] using disruptive technologies that comply with the spirit and original intent of the Internet. The Internet is a commons with its own field of operation. It's all about freedom and bringing the world together… Hacktivism is the use of technology to advance human rights through electronic media.
>
> ('The Hacktivismo FAQ v1.0')

This 'straight-faced' use of the word led to the creation of Hacktivismo, following a conversation amongst cDc members at the 2009 DEF CON hackers conference (Samuel 2004a: 90). Ruffin recruited the five core members of Hacktivismo from within and without the cDc, with the collectives aim being the creation of a tool to circumvent the state-sponsored firewalls limiting and controlling citizens' Internet

access in countries like China and Saudi Arabia. (Firewalls are Internet censorship filters acting as intermediaries between user and the rest of the Internet. When a user in a country with a national firewall enters and requests a URL or web address, the request is sent to the firewall, which checks whether the requested website is on a list of those banned by the government. If it is not, the request is then fulfilled, but if it is, the user will be sent a page conveying that the material they are trying to access is prohibited by their government.)

7.1.2 Peekabooty and the 'Hacktivismo Declaration'

The 'Peekabooty' project was the culmination of this objective - a distributed anti-censorship network application that would allow users to bypass governmental or corporate firewalls:

> …inside countries where the Web is censored... The theory behind it is simple: bypass the firewalls by providing an alternate intermediary to the World Wide Web… A user in a country that censors the Internet connects to the ad hoc network of computers running Peekabooty. A small number of randomly selected computers in the network retrieves the web pages and relays them back to the user. As far as the censoring firewall is concerned, the user is simply accessing some computer not on its "banned" list. The retrieved Web pages are encrypted using the de facto standard for secure transmission in order to prevent the firewall from examining the Web pages' contents. Since the encryption used is a secure transaction standard, it will look like an ordinary e-business transaction to the firewall.
>
> ('About the Peekabooty Project', in Samuel 2004a: 92)

Peekabooty was 'demoed' at DEF CON in 2001 as one of the conference's major highlights, (Greene 2001), but the project itself ended in abortive conflict, with its chief developer, Drunken Master (a.k.a. Paul Baranowski) leaving the Hacktivismo team and taking Peekabooty with him.

However, despite this internal ruction and the loss of the initial project itself, Peekabooty set Hacktivismo on the road of 'political coding' – indeed, they epitomise Samuel's category and she discusses them extensively (2004a). They developed and articulated a 'mission statement' for their goals and operations, which was distributed prior to the unveiling of Peekabooty, on the 4th of July, 2001. In a press release entitled "A special message of hope: An international bookburning in progress", the group outlined their dismay at the capricious and wide-ranging governmental- and corporate-led internet censorship of what they describe as "otherwise lawfully published material":

> Free speech is under siege at the margins of the Internet. Quite a few countries are censoring access to the Web through DNS [Domain Name Service] filtering. This is a process whereby politically incorrect information is blocked by domain address -- the name that appears before the dot com suffix. Others employ filtering which denies politically or socially challenging subject matter based on its content.
>
> Hacktivismo and the CULT OF THE DEAD COW have decided that enough is too much. We are hackers and free speech advocates, and we are developing technologies to challenge state-sponsored censorship of the Internet.
>
> Most countries use intimidation and filtering of one kind or another including the Peoples Republic of China, Cuba, and many Islamic countries. Most claim to be blocking pornographic content. But the real reason is to prevent challenging content from spreading through repressive regimes. This includes information ranging from political opinion, "foreign" news, women's issues, academic and scholarly works, religious information, information regarding ethnic groups in disfavor, news of human rights abuses, documents which present drugs in a positive light, and gay and lesbian content, among others […]
>
> We are sickened by these egregious violations of information and human rights. The liberal democracies have talked a far better game than they've played on access to information. But hackers are not willing to watch the custodians of the International Convention on Civil and Political Rights and the Universal Declaration of Human Rights turn them into a mockery. We are willing to put our money where our mouth is.
>
> Hacktivismo and the CULT OF THE DEAD COW are issuing the HACKTIVISMO DECLARATION as a declaration of outrage and a statement of intent. It is our Magna Carta for information rights. People

> have a right to reasonable access of otherwise lawfully published information. If our leaders aren't prepared to defend the Internet, we are.
>
> ('A special message of hope' 2001)

The press release then reproduced the Hacktivismo declaration in full. This declaration will be dealt with in detail within the textual section of the analysis, but some introductory discussion of it is merited here. As the cDc and Hacktivismo have themselves summarised, it is a document that condemns state-sponsored censorship of the Internet, with the primary objective of "*[g]etting some sort of discussion going* around information rights" (emphasis added) – a significant statement considering the analytical focus on the group's counterpublicity. The document cites Article 19 of the Universal Declaration on Human Rights (which has previously been discussed in terms of Internet rights as fundamental human rights) and Article 19 of the International Covenant on Civil and Political Rights, both of which are "internationally recognized documents that equate access to information with human and political rights". Hacktivismo also state "unequivocally that reasonable access to lawfully published material on the Internet is a basic human right; that [they are] disgusted with the political hypocrisy and corporate avarice that has created this situation" and that they are going to "step up to the plate" and do something about it ('The Hacktivismo FAQ v1.0').

As stated in 'A special message of hope' (2001), this "lawfully published material" includes such things as political opinions, international news, information on women's rights, academic and scholarly texts, religious opinions, information regarding human rights abuses, and gay and lesbian content. They do recognise that some information should be restricted, but, in line with the hacker ethic (Levy 1984), believe that most information wants to (and indeed, should be) free:

> Essentially [it] cuts out things like legitimate government secrets, kiddie porn, matters of personal privacy, and other accepted restrictions. But even the term "lawfully published" is full of landmines. Lawful to whom? What is lawful in the United States can get you a bullet in the head in China. At the end of the day we recognize that some

> information needs to be controlled. But that control falls far short of censoring material that is critical of governments, intellectual and artistic opinion, information relating to women's issues or sexual preference, and religious opinions. That's another way of saying that most information wants to be free; the rest needs a little privacy, even non-existence in the case of things like kiddie porn.
>
> ('The Hacktivismo FAQ v1.0')

It is interesting to note that beyond political and intellectual information and opinion, much of the material that Hacktivismo describe as 'falling far short' of being censorship-worthy falls within what has traditionally been the private realm. Hacktivismo's support for the freedom of discussion and information dissemination regarding these issues effects their meta-level transposition into the realm of the publicly political – that is, the wider political issue of informational freedom automatically catapults censored issues across the private/public boundary and into a state of public relevance.

7.1.3 Hacktivismo's projects

Following the breakdown of the Peekabooty project, Hacktivismo's "stepping up to the plate" has consisted of Ruffin directing the development of a whole new generation of anti-censorship tools, with the development team continuing to grow. The group now claims more than 40 members (Samuel 2004a: 92), including Cindy Cohn, who serves as Legal Director and General Counsel for the Electronic Frontier Foundation, a renowned international non-profit digital rights advocacy and legal organization (who was named as one of the National Law Journal's top 100 most influential American lawyers in 2006, and one of the top 50 most influential women lawyers in 2007 ('EFF's Staff')). Clearly, the group is significantly more high-powered and better connected than most hacker or hacktivist collectives, presumably due, at least in part, to Ruffin's background in public relations. They

have launched several projects over the last decade, each of which conforms to the goals stated in the 'Hacktivismo Declaration'.

7.1.3.1 Camera/Shy

Camera/Shy is a steganography tool, and was released in 2002 at the Hackers on Planet Earth (H.O.P.E) convention in 2002 as Hacktivismo's first completed project. Steganography is a subset of cryptography that involves information being encoded within image files, and Camera/Shy is a stand-alone, Internet Explorer-based web browser that interprets and displays information hidden within .gif image files – as Ruffin stated "You can hide pretty much any digital content in a digital image. You can have a picture of Jiang Zemin, and you can hide a picture of the Dalai Lama in it" (Einhorn 2002). Like Peekabooty, it was developed for "democracy activists operating from behind national firewalls", and "allows users to trade in banned content across the Internet":

> Sometimes hiding the truth is the best way to protect it, and yourself. Designed with the non-technical user in mind, Camera/Shy's "one touch" encryption process delivers banned content across the Internet in seconds. Utilizing LSB steganographic techniques and AES-256 bit encryption, this application enables users to share censored information with their friends by hiding it in plain view as ordinary gif images.
>
> Camera/Shy is the only steganographic tool that automatically scans for and delivers decrypted content straight from the Web. It is a stand-alone, Internet Explorer-based browser that leaves no trace on the user's system. As a safety feature Camera/Shy also includes security switches for protection against malicious HTML. Picture that.
>
> (Katt 2002)

Camera/Shy was released as open source, under the GNU General Public Licence, and is dedicated to Wang Ruowang, a Chinese dissident. Hacktivismo have received

emails from users in Iran, China, and the United Arab Emirates, thanking them for distributing Camera/Shy (Einhorn 2002; Ruffin 2004b, in Samuel 2004a: 188)

7.1.3.2 The Six/Four System

The Six/Four System, named for the date of the Tiananmen Square massacre, was released in 2003, and is similar to Peekabooty in that it allows users to circumvent firewalls by 'tunneling' through them. It uses 'trusted peers' or intermediaries, who provide a securely encrypted relay mechanism for users to get through to censored content. Because it uses strong encryption, and the US government regulates the export of cryptography tools, Hacktivismo went through the process of obtaining US government approval, with Six/Four thus becoming the first product of a hacker group to be granted such approval.

7.1.3.3 The Hacktivismo Enhanced-Source Software License Agreement (HESSLA)

Hacktivismo also created a software licence agreement as a corollary to the Six/Four System, which was written by Ruffin and Eric Grimm, an attorney with the Electronic Frontier Foundation. The Hacktivismo Enhanced-Source Software Licence Agreement (HESSLA) was inspired by the GNU General Public Licence, the most used free software licence. The HESSLA is a legal agreement that is intended to bind the users and modifiers of software licensed under it to certain political terms of use – namely, that they do not use or modify the software to violate human rights or spy on other users. The Free Software Foundation have criticised it as due to these ethical restrictions, it is no longer technically a free

software licence, and as a copyright based source licence, restrictions on its use are not legally enforceable ('The HESSLA's problems'). However, Ruffin has stated that Hacktivismo will be satisfied if they "deter at least some of the 'evil-doers' from using [their] software" (Ruffin 2004b, in Samuel 2004a: 96).

7.1.3.4 Scatterchat

ScatterChat was released in 2006, under the HESSLA, and is again a project intended for "non-technical human rights activists and political dissidents operating behind oppressive national firewalls" ('ScatterChat Press Release' 2006). It is a secure instant messaging or chat client, and provides encryption and secure file transfers through integration with Tor. Tor is an 'onion router' (indeed, Tor stands for 'The Onion Router'), which creates a network of encrypted 'tunnels' that are resistant to 'traffic analysis' (which uses packet data to infer who is talking to whom over a given network). As the Tor Project explains:

> The idea is similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you — and then periodically erasing your footprints. Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several relays that cover your tracks so no observer at any single point can tell where the data came from or where it's going.
>
> ('Tor: Anonymity online')

As such, ScatterChat is designed to allow users such as human rights activists and political dissidents to communicate anonymously and securely in hostile environments. As described by the lead developer, "[t]he anonymity and encryption that ScatterChat provides ensures that both the identities and messages of activists remain a mystery, even to well-funded totalitarian governments." ('ScatterChat Press Release' 2006).

7.1.3.5 Torpark or the XeroBank Browser

Torpark (v.1.5.0.7) also utilises Tor, and was also released in 2006 under the GNU General Public Licence in 2006 as a joint cDc/Hacktivismo project with Steve Topletz. The current iteration of the browser (v 3.9.10.24) is now called XeroBank (xB), and is developed by Topletz, after being rebuilt from the ground up in 2007. Torpark and xB are highly modified variants of the Firefox Portable web browser, and can be run from portable media such as USB flash drives, or on internal hard drives. They use Tor to anonymise the connection between the user and website being visited. Torpark is dedicated to the Panchen Lama, in a nod to China's continued persecution of and interference with the Tibetan spiritual leader's dynasty. Like the other Hacktivismo projects, it is intended to protect users from hostile governments and data thieves, as its press release explains:

> "We live in a time where acquisition technologies are cherry picking and collating every aspect of our online lives," said Hacktivismo founder Oxblood Ruffin. "Torpark continues Hacktivismo's commitment to expanding privacy rights on the Internet. And the best thing is, it's free. No one should have to pay for basic human rights, especially the right of privacy."
>
> ('Hacktivismo releases Torpark for anonymous, portable web browsing' 2006)

7.1.4 Hacktivismo and the cDc today

Hacktivismo have been quiet in the last few years, but most of their software is still freely available on open source software hosting sites such as SourceForge ('SourceForge'). The cDc are still very much alive, as the activity on their website and public 'Bovine Dawn Dojo Forum' attests. They also released the 'Goolag

Scanner' in 2008, a web auditing tool that uses Google to check websites for security vulnerabilities so that they may be patched:

> "It's no big secret that the Web is the platform," said cDc spokesmodel Oxblood Ruffin. "And this platform pretty much sucks from a security perspective. Goolag Scanner provides one more tool for web site owners to patch up their online properties. We've seen some pretty scary holes through random tests with the scanner in North America, Europe, and the Middle East. If I were a government, a large corporation, or anyone with a large web site, I'd be downloading this beast and aiming it at my site yesterday. The vulnerabilities are that serious."
>
> (Katt 2008)

Ruffin continues to be an active spokesperson for Internet-based human rights, speaking out over the planned extradition of the 'Pentagon hacker', Gary McKinnon (McKinnon suffers from Asperger's Syndrome and clinical depression, and Ruffin and McKinnon's supporters argue that extradition is a disproportionate response to his crimes (which he committed while looking for evidence of UFOs) and is likely to severely impact his mental health, with possibly fatal consequences) (Ruffin 2009). He is an active presence on Twitter (@OxbloodRuffin), and continues to criticise governments such as those of China and Iran for violating their citizens' human rights, as well as those corporations and Western governments who either profit from these violations or stand idly by (Ruffin 2009b), and lauds the use of Tor and other technologies that have allowed the Iranian people to speak out about the recent election and quashed rebellion.

7.1.5 Hacktivismo's constellation of publics

Hacktivismo can plainly be understood as a hacktivist counterpublic, using the neo-Habermasian lense developed in the preceding chapter. Cohering around the issue

of online freedoms and the opposition of censorship, they clearly outline their intent to mobilise their ideological discourse and generate discussion and deliberation through their Declaration and software projects – as quoted, they want to get through their FAQ objective of "*[g]etting some sort of discussion going* around information rights" (emphasis added) ('The Hacktivismo FAQ v1.0'). We may confidently assume that their intent is to provoke those who encounter their discursive publicity into reflection on their political preferences with regards to internet censorship, and as an analysis of their Declaration reveals, they invest a considerable amount of effort into attempting to convert this reflection in preference alteration in support of their point of view. Their activities are non-violent and non-coercive, and are, in fact, intended to free repressed citizens from the coercive and repressive regimes they exist within. The following analysis extends upon this neo-Habermasian interpretation, and explores the specific ways in which they effect their counterpublicity and thus attempt to threaten or fracture the dominant or hegemonic structures they oppose.

7.1.5.1 Repressive regimes

We can best conceive of Hacktivismo (and, indeed, any public or counterpublic) as existing in relation to what we imagine as a constellation of other publics, not just one singular public. The primary dominant or hegemonic 'publics' Hacktivismo intend to counter are the generally authoritarian governments or 'repressive regimes' involved in censoring their citizens' free and unhindered access to the Internet, through the use of firewalls and surveillance technology. Of course, these regimes do not really constitute national publics at all – they hark back to the feudal structures pre-dating Habermas's bourgeois public sphere. They display their publicity before their people and the rest of the world, claiming to speak for them and their best interests, and denying them the rights of unhindered self-expression and self-determination. They police the submission of their citizens through censorship and surveillance technologies that either directly obstruct their digital freedoms or generate an online panopticon – a self-disciplining climate of fear

where people submit to repression and 'toe the line' for fear of harsh reprisal if they behave otherwise. As such, they are best described as pseudopublics rather than true publics.

All of Hacktivismo's projects are oriented towards helping citizens resist and escape from this kind of censorship and surveillance, and they make this goal explicitly clear in their project descriptions and press releases. These repressive regimes are primarily identified as those considered by Reporters Sans Frontières (RSF) (and other watchdog organisations) as 'Enemies of the Internet', and are, for the most part, authoritarian and/or communist states such as China, Iran, Cuba, and North Korea ('Reporters Sans Frontières'). Any government practicing online surveillance that leads its citizens to self-censor either the discourse they seek or the discourse they express online, or that directly censors and controls what Hacktivismo define as the 'lawfully published material' their citizens may have access to, is a dominant or hegemonic pseudopublic whose stability and control Hacktivismo intend to call into question and destabilise through their hacktivist counterpublicity.

As part and parcel of this, their counterpublicity is also oriented towards the transnational but geographically based technology corporations that aid these repressive regimes in their censorship and human rights violations. These corporations are search and web service corporations and service providers such as Google, who self-censored their Google.cn domain at the request of the Chinese government, and have only recently ceased this operation, and only after suffering Chinese hacker attacks on their own servers and intellectual property. Continuing examples are Microsoft's Bing and Yahoo! Search (which is powered by Bing) who continue to censor their Chinese operations in line with Beijing's directives. They also include hardware corporations such as Cisco (America), Nokia (Finland), and Siemens (Germany), who have provided firewall and surveillance technologies to China (Cisco) and Iran (a joint venture between Nokia and Siemens, quite possibly because American firms are not allowed to trade with Iran) (Ruffin 2009; Rhoads & Chao 2009; Zeller 2006). Ruffin describes these corporations as "Gadarene swine…Already fat and greedy beyond belief, the Western technology titans are being herded towards the trough" (Ruffin 2002). These corporations arguably do not constitute publics or even pseudopublics in and of themselves, as they have no

detailed ideology beyond the neo-liberal political-economic ideology of the profit motive *über alles* - but they provide the essential technological support mechanisms for the dominant national governmental publics or repressive regimes, and as such, are implicated in and critiqued by Hacktivismo's counterpublicity against these regimes.

7.1.5.2 Hypocritical Western governments

Hacktivismo perceive the next level off involvement to be constituted by those liberal Western governments, such as those of America and various European nations, who sanction or condone these corporate actions and the repression they effect through remaining silent, while simultaneously and publicly decrying the repressive regimes these corporations support - liberal governments who are described by Hacktivismo as having "talked a far better game than they've played on access to information" ('A special message of hope' 2001). This "governmental douchebaggery" (Ruffin 2009) is seen as not only hypocritical and amoral but also a threat to global security, in that it perpetuates the existence of repressive and unstable states within the international community:

> With billions of dollars in government budgets at their disposal, when are the world's liberal democracies going to put some of their resources into opening up the Internet? We know they don't care about human rights policy when it conflicts with jobs at home; but what about international security? As Beijing continues to play the patriotism card domestically, a more open Internet could diffuse traditional xenophobia through greater one-on-one interaction on-line.
>
> (Ruffin 2002)

Hacktivismo clearly see these liberal governments as being in political-economic collusion with these technology corporations – ignoring their distasteful activities for the sake of their domestic economies and the profit coming in from the

totalitarian governments who are commissioning the construction of firewalls and surveillance technology. Operating under the same neoliberal objectives as the corporations, these governments wordlessly accept the 'dirty money' flowing into their economies from the systems of global capitalism, while simultaneously and vocally castigating the sources of this revenue for the maltreatment of their citizens. Once again, they are more pseudopublics than true publics – they parade their support for informational freedoms and human rights in front of their domestic voting and international publics to win support and 'buy' legitimacy, while prioritising their corporations' bottom lines above any practical or effortful upholding of these democratic ideals. They parade their democracy before the people, but fail to actually endorse it at an international and conceptual level.

Furthermore, these governments themselves are certainly not innocent of attempting to regulate and control the Internet. The current global governmental negotiations regarding the installation of the Anti-Counterfeiting Trade Agreement (ACTA) are a notable current example. ACTA seeks to establish international standards on the enforcement of intellectual property rights, particularly those regarding Internet copyright infringement, and its negotiations have (like so much media regulation) been cloaked in secrecy and lacking in any true democratic accountability to the citizens of the nations involved. Cognizant of this kind of behaviour, Hacktivismo are quick to remind us that we should also be worried about our own governments, and the trends towards governmental control of the Internet in general:

> Q: Who cares if Iraq or Cuba censors the Internet? It ain't nothin' to me.
> A: Substitute the word control for censor. The fact that dictators are ham-fisted and obvious is only a testament to their arrogance and contempt for humanity. All governments want to control the Internet in one form or another. The United States, Germany, France, the United Kingdom, and Australia - just to name a few - have all enacted legislation governing use of the Internet, some of it very bad.
>
> ('The Hacktivismo FAQ v1.0')

7.1.5.3 The global citizenry, or dispersed global 'public of publics'

This reminder that it is not only authoritarian states that are practicing Internet censorship and surveillance, and that Western citizens should 'keep an eye on' their own governments, speaks to a wider global and non-specific 'public of publics' of Internet users that Hacktivismo wish to engage with – a concept more easily grasped and even visualised if we recall Keane's theorized 'global modular network' of public and counterpublics, operating at multiple (micro-, macro- and meso-) levels (2000). This aspect of the neo-Habermasian model is also useful for imagining the wider constellation of publics that Hacktivismo exists in relation to, including those of the repressive regimes, technology corporations and liberal governments. Coming up with any concrete explanation or visualization of this highly interconnected network of publics, both counter- and pseudo-, is a task beyond this thesis's reach, but as long as can understand that this constellation is both networked, multivalent, and dynamic, Keane's rather elegant theory has fulfilled its purpose.

As previously elucidated, Hacktivismo's desire to provoke political preference reflection amongst a dispersed global citizenry is made explicitly clear in the explanation provided for their Declaration:

> Hopefully people will read it and think it's a good thing, or a total piece of crap. Getting some sort of discussion going around information rights is the primary objective.
>
> ('The Hacktivismo FAQ v1.0')

They aspire to incite a wider public discourse about Internet censorship and "information rights" – to have more people join the debate over the freedom of information and discursive expression on the Internet. Indeed, mobilising their ideological discourse into wider publicity and thus catalyzing discussion and

deliberation within the dispersed global public of publics is their 'primary objective' – one could argue that they are a textbook case of a self-aware and externally oriented counterpublic. They thus enact Calhoun's argument for the importance of interpublicity (1997: 81) – that counterpublic discourses must traverse across basic lines of difference and engage with other publics in order to truly fulfil their externally-oriented component.

Obviously, they seek to not only inform and provoke political preference reflection amongst this non-specific agglomeration of citizens, but to (hopefully) convert some of these citizens into supporters of their cause (although they do recognise the inevitability of a plurality of positions through their statement that some may think their Declaration is a "total piece of crap", seemingly agreeing with Dryzek about the centrality of argument to deliberation and political preference reflection (2000)). Their counterpublicity (in terms of its constitutive discourse or ideology, if not form) is intended to be self-replicating or viral, through provoking not just contestation and political preference reflection but also political reference alteration. That is, they do not necessarily want more members for Hacktivismo, but they want others to support the ideology Hacktivismo enacts counterpublicity in aid of - to "think it's a good thing" and to mobilise some form of public support for it - and thus become part of a wider and agglomerative 'public of counterpublics' opposed to the curtailment of Internet based information rights. This public of counterpublics, by virtue of each public's shared core ideology, would be linked by 'chains of equivalence' (Laclau & Mouffe 1985), and thus the discursive strength or counterpublicity that each public brings to bear on the dominant publics would be amplified – the public of counterpublics will be more than the sum of its parts.

We can therefore see that Hacktivismo, as a counterpublic constituted by a general discourse in support of Internet-based information rights as part and parcel of the wider maintenance of human rights, are committed to attempting to destabilize or threaten the cohesion of two categories of dominant public: primarily, the specific, nationally dominant state publics of repressive regimes and of hypocritical Western governments, as well as the corporate publics sanctioned by Western governments and aiding the repressive regimes in their censorship. They are also attempting to provoke political preference reflection within a more dispersed global public of

publics, in the hope of engendering the formation of a wider public of counterpublics, collectively sharing and amplifying Hacktivismo's catalytic counterhegemony.

7.2 Text

Having identified these targets and goals, we may explore how exactly Hacktivismo's counterpublicity attempts to achieve them. Hacktivismo have obviously produced many texts to accompany their projects, in the form of press releases, media statements, and general website material and news. However, as previously stated, the 'Hacktivismo Declaration' is the discursive matrix for almost all of these secondary materials. Most of the press releases accompanying their software paraphrase it, and these press releases also direct readers to Hacktivismo's webpage, where the Declaration is both reproduced in full, and paraphrased throughout the various sections of their website. The Declaration is a purposefully expressed, coherent, formal system of belief – an 'intellectual' as opposed to 'lived' ideology (Billig *et al* 1988, in Barker & Galasinski 2001). It comprehensively defines Hacktivismo's counterpublicity through discourse, and as such, is the logical text for critical linguistic analysis. It is reproduced in full below, preserving original formatting, with reference/paragraph numbering added in bold:

> THE HACKTIVISMO DECLARATION
>
> assertions of liberty
> in support of an uncensored Internet
>
> DEEPLY ALARMED that state-sponsored censorship of the Internet is rapidly spreading with the assistance of transnational corporations, **(1)**
>
> TAKING AS A BASIS the principles and purposes enshrined in Article 19 of the Universal Declaration of Human Rights (UDHR) that states, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and

regardless of frontiers", and Article 19 of the International Covenant on Civil and Political Rights (ICCPR) that says, **(2)**

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

a. For respect of the rights or reputations of others;
b. For the protection of national security or of public order, or of public health or morals. **(3)**

RECALLING that some member states of the United Nations have signed the ICCPR, or have ratified it in such a way as to prevent their citizens from using it in courts of law, **(4)**

CONSIDERING that, such member states continue to willfully suppress wide-ranging access to lawfully published information on the Internet, despite the clear language of the ICCPR that freedom of expression exists in all media, **(5)**

TAKING NOTE that transnational corporations continue to sell information technologies to the world's most repressive regimes knowing full well that they will be used to track and control an already harried citizenry, **(6)**

TAKING INTO ACCOUNT that the Internet is fast becoming a method of repression rather than an instrument of liberation, **(7)**

BEARING IN MIND that in some countries it is a crime to demand the right to access lawfully published information, and of other basic human rights, **(8)**

RECALLING that member states of the United Nations have failed to press the world's most egregious information rights violators to a higher standard, **(9)**

MINDFUL that denying access to information could lead to spiritual, intellectual, and economic decline, the promotion of xenophobia and destabilization of international order, **(10)**

CONCERNED that governments and transnationals are colluding to maintain the status quo, **(11)**

DEEPLY ALARMED that world leaders have failed to address information rights issues directly and without equivocation, **(12)**

RECOGNIZING the importance to fight against human rights abuses with respect to reasonable access to information on the Internet, **(13)**

THEREFORE WE ARE CONVINCED that the international hacking community has a moral imperative to act, and we **(14)**

DECLARE:

THAT FULL RESPECT FOR HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS INCLUDES THE LIBERTY OF FAIR AND REASONABLE ACCESS TO INFORMATION, WHETHER BY SHORTWAVE RADIO, AIR MAIL, SIMPLE TELEPHONY, THE GLOBAL INTERNET, OR OTHER MEDIA. **(15)**

THAT WE RECOGNIZE THE RIGHT OF GOVERNMENTS TO FORBID THE PUBLICATION OF PROPERLY CATEGORIZED STATE SECRETS, CHILD PORNOGRAPHY, AND MATTERS RELATED TO PERSONAL PRIVACY AND PRIVILEGE, AMONG OTHER ACCEPTED RESTRICTIONS. BUT WE OPPOSE THE USE OF STATE POWER TO CONTROL ACCESS TO THE WORKS OF CRITICS, INTELLECTUALS, ARTISTS, OR RELIGIOUS FIGURES. **(16)**

THAT STATE SPONSORED CENSORSHIP OF THE INTERNET ERODES PEACEFUL AND CIVILIZED COEXISTENCE, AFFECTS THE EXERCISE OF DEMOCRACY, AND ENDANGERS THE SOCIOECONOMIC DEVELOPMENT OF NATIONS. **(17)**

THAT STATE-SPONSORED CENSORSHIP OF THE INTERNET IS A SERIOUS FORM OF ORGANIZED AND SYSTEMATIC VIOLENCE AGAINST CITIZENS, IS INTENDED TO GENERATE CONFUSION AND XENOPHOBIA, AND IS A REPREHENSIBLE VIOLATION OF TRUST. **(18)**

THAT WE WILL STUDY WAYS AND MEANS OF CIRCUMVENTING STATE SPONSORED CENSORSHIP OF THE INTERNET AND WILL IMPLEMENT TECHNOLOGIES TO CHALLENGE INFORMATION RIGHTS VIOLATIONS. **(19)**

The Hacktivismo declaration works to not only declare Hacktivismo's intellectual ideology to readers, but to provoke political preference reflection that will hopefully result in both sympathy for their cause and actions, and disapproval and dissent against the dominant publics they aim to counter. It functions as a detailed elucidation of the counterpublicity embedded within their software projects; that is,

the text distills the intent behind the form of their hacktivism. It does this by categorically identifying and negatively characterising the dominant publics against which Hacktivismo is oriented, and by constructing a positive self-presentation for Hacktivismo themselves.

7.2.1 Identification and negative characterization of dominant publics through text

The repressive regimes against which Hacktivismo orient their counterpublicity are identified in a non-specific manner within the Hacktivismo Declaration, in keeping with the fact that they are numerous, and they are all perceived as equally reprehensible. Rather than speaking of specific "states sponsoring censorship", the Declaration utilizes nominalisation, transforming the representation of the multiple processes or actions of censorship by specific states into a noun, or a thing. This noun, "state-sponsored censorship of the Internet", is used four times within the declaration (in paragraphs 1, 17, 18 and 19), thus underlining Hacktivismo's focus towards it as their main bone of contention. This nominalisation of the process of censorship and repression and general use of non-specific nouns also occurs in other forms, such as "the world's most repressive regimes" (6), "some countries" (8), "the world's most egregious information rights violators" (9), "human rights abuses" (13), "the use of state power to control access" (16), and "information rights violations" (20).

We can interpret these constructions as being both efficient, in that they mean that Hacktivismo do not have to identify each and every repressive regime against which they are oriented, and in that it means that the Hacktivismo declaration will not require future revisions to ensure that it remains current (if more states begin to practice Internet censorship or if some currently doing so cease and desist). However, it also highlights the fact that Hacktivismo are oriented primarily against a particular kind of national discourse or public – they are not opposed to specific national publics per se, but to governing pseudopublics which fulfill a particular

criteria or who do a particular action. They are pursuing a cause, not a specific nation or nations. Their counterpublicity is primarily oriented towards a particular kind of discursive abuse – that is, a particular process - and secondarily, and by extension, towards those national pseudopublics or repressive regimes which enact this abuse.

This efficient non-specificity is continued through the use of collective nouns and nominalisations such as "member states of the United Nations" (4, 5, 9), "the assistance of transnational corporations" (1), "transnational corporations" (6), "governments and transnationals" (11), and "world leaders" (12). At no point in the declaration is a specifically named actor singled out – Hacktivismo identify diverse and unnamed actors as dominant publics or supportive agents against which they are oriented by what they do, rather than who they are. (However, one might argue their dedication of pieces of their software to Chinese dissidents and a Panchen Lama signals a significant focus on China as their 'most wanted' repressive regime.)

Furthermore, Hacktivismo repeatedly characterise what these dominant publics do – that is, their censorship of the Internet - as exceptionally negative. Repressive regimes, with the assistance of technology corporations: "have signed the ICCPR [International Covenant on Civil and Political Rights], or have ratified it in such a way as to prevent their citizens from using it in courts of law" (4), they "continue to willfully suppress wide-ranging access to lawfully published information on the Internet, despite the clear language of the ICCPR that freedom of expression exists in all media" (5), and they "track and control an already harried citizenry" (6). The adverb "willfully" indicates that they purposively deny their citizens access to material that they are legally allowed access to, and in doing so, ignore, defy or subvert an internationally agreed-upon covenant, thus breaching human rights and breaching the rules of a wider global citizenship. In doing so, Hacktivismo invite us to see these regimes as both arrogant, in that they seem to believe that they are entitled to operate outside the bounds of these international treaties; and as rogue-states, operating outside the bounds of international law and thus delegitimizing themselves within or ex-communicating themselves from the international community, and from all the benefits that this community-belonging confers.

Despite this being a rather toothless notion (as China certainly continues to enjoy all the benefits of a globalised economic system, as do other such regimes), it certainly does considerable work towards establishing these kinds of states as 'other', as not belonging, and therefore being both threatening and alien.

Hacktivismo also see these repressive regimes as akin to hunters - they track and control their citizens as if they were prey, cruelly denying them freedom and agency and worsening the stress and persecution they have already inflected upon them. The adverb "already" signals to the reader that this censorship is a continuation of a history of abuse and repression, simply the latest episode in a procession of violations. The use of the possessive pronoun "their", and of material clauses utilising the verbs "suppress", "track" and "control", indicate that these regimes have ownership over the citizens in their nations, and can do with them what they will. The fact that what they choose to do, and to do knowingly, is to inflict severe and unpleasant restrictions upon their citizens elaborates upon the discourse of othering through explicitly delineating the cruelty and inhumanity characterising the governing bodies of these regimes.

Hacktivismo paint the effects of this censorship in even more vivid terms. Initially, they merely hypothesise, through the use of the modal auxiliary "could" (10), that "denying access to information could lead to spiritual, intellectual, and economic decline, the promotion of xenophobia and destabilisation of international order" (10). However, this lone instance of supposition is soon discarded in favour of assertions of facticity. Internet censorship "erodes peaceful and civilised coexistence, affects the exercise of democracy, and endangers the socioeconomic development of nations" (17); "is a serious form of organised and systematic violence against citizens, is intended to generate confusions and xenophobia, and is a reprehensible violation of trust" (18). The material clauses utilising such verbs as "erode" and "endanger" make a factual claim that Internet censorship is a destructive force. It is dramatized as a corrosive substance that destroys or eats away at a multitude of positive abstract nouns - peace, civilization, democracy, socioeconomic development and trust, with the only things it actually "generates" or gives birth to rather than destroys being the negative abstract nouns of confusion and xenophobia. It destroys all that is desirable and civilised and fosters only

disorder, hatred and fear. The reader is presented with an image of the chaotic, hellish existence that would result from the widespread application of such censorship, and of the national hells that it has already spawned.

The adjectives "organised" and "systematic", as well as the verb "intend" underline the purposive nature of this destruction and chaos - censorship is a direct and intentional affront to democracy and to global harmony and prosperity. The repressive states engaging in Internet censorship know the negative consequences of their behaviour, but do not care, and perhaps even revel in them. The Declaration also describes state-sponsored Internet censorship as "violent" and "reprehensible", both exceedingly strong adjectives that further emphasize the destruction occurring and the need for our concern and censure, through grounding and amplifying our impression of its severity with connotations of forceful physicality.

Hacktivismo also describe the alterations and subversions these repressive regimes have wrought on various specific aspects of the world in terms of corruption and degradation. They have turned the Internet into "a method of repression rather than an instrument of liberation" (7), and made it "a crime to demand the right to access lawfully published information, and of other basic human rights" (8). Hacktivismo thus characterise the actions of repressive states as cancerous forces, infecting good things and actions and corrupting them into their binary opposites. What was once a freeing, emancipatory technology is distorted into a tool for repression, and the legal assertion of one's basic human rights is inverted into a criminal act. Hacktivismo's description of Internet censorship as "rapidly spreading" (1) extends these connotations of cancer and malignancy – it is a virus, out of control and capable of global infection if we do not do something to halt its progression.

The unspecified transnational corporations supplying censorship technology are also strongly negatively characterised, as they "assist" (1), and "continue to sell" (despite "knowing full well" the consequences) (6) their wares to these destructive regimes. They do not merely provide the tools for censorship; they help to install it, with the purposive connotations of "assist" underlined by their knowledge of what they are doing. They are the willing and informed helpers of destruction and corruption, privileging profit over human rights and morality. They are encouraged by, and take advantage of global neoliberal policies that have removed most

boundaries to global trade, and export their software and hardware to anywhere that will turn them a profit. Paired with these traitorous corporations are other UN member state governments and "world leaders" (12) who repeatedly "fail" to do anything, let alone anything timely, to help (9, 12), and who are thus involved with both the repressive regimes and the transnational corporations in "colluding" (11) – purposefully and deviously co-operating – to maintain the "status quo" (11) of governmental and corporate dominance. Thus their description as "world leaders" is rendered ironic; they are not leaders but failures.

Through this series of negative characterisations, Hacktivismo bundle together the three categories of pseudopublic they have identified as adversaries, with the discursive work done to condemn each thus also working to infect the others by proximity and association. They are established as an overarching entity or 'public of pseudopublics' to be opposed, with Hacktivismo clearly orienting themselves and their counterpublic discourse towards their opposition and destabilisation – they comprise a powerful political-economic hegemony that Hacktivismo are very much invested in threatening and hopefully fracturing.

7.2.2 Positive characterization of Hacktivismo through text

Hacktivismo's negative characterisation of these hegemonic pseudopublics is counterpoised by the textual work they do to characterise themselves in a positive light, and thus worthy of support. Indeed, the very nature of the Hacktivismo Declaration, composed as it is by a series of formal declarative statements, works to establish Hacktivismo as a figure of authority – they speak to us, and we listen. (This, of course, also has the effect of grounding their negative characterisation of the dominant publics in an impression of reputability). This air of authority is deepened by the intertextual components of the Declaration. They have not only borrowed from the discursive form or 'speech genre' (Bakhtin 1986) of a formal legal declaration, with its connotations of trustworthiness and authority, but have actually reproduced components of two extremely well-known and well-regarded

legal declarations on informational and expressive rights (Article 19 of the Universal Declaration of Human Rights, and Article 19 of the International Covenant on Civil and Political Rights) and "taken them as the basis" for their own declaration (2, 3). The placement of this intertextual component in the first section of the Hacktivismo Declaration immediately works to give the reader the impression that Hacktivismo are a serious and principled group of individuals, cognizant of and well-versed in international law, and thus worthy of our attention and consideration. This impression is prefigured by the gravitas of the document's subtitle – the rather grand sounding "assertions of liberty in support of an uncensored Internet". By aligning themselves with these tenets of international law, and by working to confer an air of authority upon their discourse, Hacktivismo seek to instill their counterpublic with some modicum of power – a strategy that is also helped through their diverse membership, which includes well-regarded and prominent legal professionals. Downey's reminder that counterpublics may actually include some relatively powerful participants (2007) is extremely pertinent in this case.

Hacktivismo continue this positive self-presentation and claim to power with the stream of active declarations utilising mental and behavioural processes that comprise the structural frame of the first section of the declaration (1-14). They have removed themselves from these framing clauses – rather than saying "We are deeply alarmed", they omit the personal pronoun "We", leaving the reader to make the logical assumption that it is indeed Hacktivismo who are declaring these things, as it is, after all, their declaration. It also depersonalizes their discourse, with the effect of it assuming a more disemobodied and rational air of authority – they are, in fact, engaging in what Warner calls self-abstraction (2002), removing their personal identities from their discourse in favour of a rational-critical approach. Due to the relatively powerful and educationally privileged nature of their membership, they are capable of mobilising this kind of differentially distributed mode of communication.

This, in combination with the capitalization of these mental and behavioural processes, serves to highlight the thoughtful and serious cognitive work that Hacktivismo are doing in constructing and expressing their intellectual ideology.

They are “recalling” (4, 9); “considering” (5); “taking note” (6); “taking into account” (7); “bearing in mind” (8); and “recognizing” (13). Furthermore, they are “deeply alarmed” (1, 12); “mindful” (10); and “concerned” (11). Clearly, this declaration is not something that they have taken lightly – they have been monitoring and mulling over the increasing “state-censored sponsorship of the Internet”, doing extensive mental and intellectual work, and the subject is something they care deeply about and are seriously engaged with. Their conviction that “the international hacking community has a moral imperative to act” – to oppose and resist this censorious behaviour rather than failing to act like the “world leaders” have (12) – is self-inclusive, and prefigures the course of action they propose in the second section of the declaration.

They continue to present themselves as thoughtful and serious in the second section of the declaration (15-19), in which they explicitly identify themselves with the pronoun “we” (16, 19). This section is also fully capitalized, again drawing attention to Hacktivismo as the active authors of the document. Their declaration that “full respect for human rights and fundamental freedoms includes the liberty of fair and reasonable access to information” (15) implicitly informs us that they, in contrast to those actors involved in censoring the Internet, do have full respect for human rights and fundamental freedoms – they are the ones reminding or informing us of what this respect involves, thus placing themselves in a position of moral responsibility and authority. Their “recognition” that governments do have to impose some “acceptable restrictions” on what information their citizens have access to shows us that they are reasonable and considerate individuals – they are not reacting out of pure anti-authoritarian sentiment but out of a genuine concern about censorious behaviour that goes beyond the pale. They use the pronoun “we” in identifying their opposition to the ‘unreasonable’ censorship of “the works of critics, intellectuals, artists, or religious figures”, thus underlining the personal investment they have in opposing this limitation of human endeavour and expression (16).

This positive self-representation as thoughtful, concerned, personally invested, and morally and intellectually authoritative individuals provides the raison d'être for the course of action Hacktivismo propose in the final paragraph of the declaration.

They will "study" (with its connotations of industriousness and academic integrity) "ways and means of circumventing state sponsored censorship of the Internet" and will "implement technologies' (which carries connotations of cleanness and efficiency) to "challenge information rights violations" (19). They will invest time and effort in researching and creating various technological fixes to counter the Internet censorship of repressive regimes, thus signaling to the reader that they are hard working and genuinely invested in this issue. In the absence of any other individuals in positions of responsibility 'stepping up' and fulfilling their responsibilities by doing something about the destructive and regressive practice of state-sponsored Internet censorship, Hacktivismo let us know that they are going to be the ones who 'do the right thing', and take action to oppose this reprehensible activity, and those who perpetrate it. They are clearly the heroes of the declaration, and the governments (both repressive and impotent) and corporations are the villains.

Hacktivismo thus definitely establish the positive self-presentation of their counterpublicity and negative other-presentation of the dominant pseudopublics of repressive regimes and hypocritical Western governments through the textual component or content of their hacktivism. However, it is through the form of their hacktivism, and its 'hacking' or subversion of the dominant patterns of access to or power over discourse that they launch this textual component into wider circulation.

7.3 Access and control

7.3.1 Code is speech

Before we explore these subversions of access and control, a quick word must be said about the status of Hacktivismo's software as discourse capable of being analysed. Conducting a discourse analysis of this software may seem impossible. While programming code does indeed share many attributes with written text, in

that it comes in different languages, and has what can be understood as lexico-grammatical and lexical components, it clearly cannot be subjected to an analysis based on systemic-functional linguistics, not does it have images or other readily interpretable semiotic elements. However, Hacktivismo's projects can be understood as both the embodiment of and delivery mechanism for the central ideology expressed in their declaration, and as such, are an integral component of Hacktivismo's hacktivist discourse.

In line with this, there is a strong argument for understanding source code as a form of speech. The FLOSS movement (one of the generations of hackers, as we have already discussed, and one who share close evolutionary ties with hacktivism, in that they are both politically engaged) has and continues to assert that not only is code a form of speech, it is entitled to the same protection as free speech. This code/speech association has stabilized as the result of the FLOSS movement's recent constitutive resistance to the "excessive copyrighting and patenting of computer software", but programmers or hackers have been making the connection since the early nineties (Coleman 2009: 433). There is no room to go into great detail here (although the topic is a fascinating one), but in summary, what had existed as an implicit claim was made explicit through the FLOSS movement's involvement in several court cases hinging on the assertion that source code equates to speech, and should therefore be legally protected as such. Although code was not found deserving of First Amendment protection in every case, it was legally accepted and established by the courts as a form of speech (ibid.: 447).

Furthermore, and quite possibly of more importance, the "arrests, lawsuits and protests [surrounding these cases] helped establish as a cultural commonplace among F/OSS [FLOSS] developers and hackers the connection between source code and speech" (ibid.: 447-448; for more detail on this issue, see also Coleman 2004). Hackers see code as speech, and therefore software programmes as texts. If the creators of a particular kind of text genuinely believe and assert that it is speech, and provide a legally accepted rationale for this assertion, then I do not believe we should contest their definition, even if we cannot read or understand the language they are speaking in. As such, we should understand Hacktivismo's programmes as texts and what they achieve as speech, and even though we may not be able to read

their source code, we can certainly comprehend and analyse what this code achieves. We can consider them as 'speech acts' or 'performative utterances' (Austin 1962) – the words and syntax used to build the programmes do not describe what they are going to do, they actually do it. When programmers write code, it is "not to *describe* [their] doing of what [they] should be said in so uttering to be doing or to state that [they] are doing it: it is to do it" (ibid.: 64). As such, we can analyse Hacktivismo's software - the non-linguistic component of their hacktivist discourse – in terms of what it does, even though we perhaps cannot read the textual forms with which they accomplish this action. That is, we can analyse Hacktivismo's various hacktivist projects in terms of how they actively subvert the dominant patterns of access to or power over political discourse.

7.3.2 Destabilising repressive regimes and provoking political preference reflection through form

In terms of countering repressive regimes and the corporations that support them, Hacktivismo's various projects serve to undermine and subvert the absolute control that these regimes have over their citizens' online engagements with and production of political discourse. These dominant pseudopublics control not only what political ideas their citizens have access to, but also the political discourses their citizens can engage in or express. In effect, they force their citizens to conform to a prescribed national politics, the limits of which are set by the government. They force their citizens to exist within a national pseudopublic (Habermas 1989) – one in which politics are displayed, but not truly participated in, because any citizens who disagree with the ideology of this dominant national public are both pre- and post-emptively silenced. These repressive regimes use corporate technology to control every aspect of their citizens' access to online political (and other kinds) of discourse, from planning, to setting, to the control of communicative events, to the scope and nature of audiences. They may only access, engage with and produce discourse and political expression when, where, and how their governments allow them to, and in front of a governmentally prescribed audience. Citizens of

repressive regimes are forced to engage with and take part in only prescribed discourses, in prescribed arenas, and with prescribed access to an audience. All their categories of access are curtailed.

Hacktivismo's various projects serve to undermine the totality of this control. They provide the citizens of repressed regimes with the means to plan their own access to and engagement with discourses that run counter the pseudopublic they are otherwise forced to be part of. They give them the ability to choose their own setting for this discursive access and expression. They allow citizens to have control over the communicative events they are a part of, in that they may access and discuss political ideologies or other modes of expression that run counter to or are censored by their national regime, and they also allow these citizens to access a wider audience for their dissident ideas, if they so wish. The recent example of Iranians using Tor-based technologies and Web proxies to access and inform a global audience (via such censored technologies as Twitter and YouTube) of the violent repression of dissident speech occurring in Iran perfectly illustrates the kind of subversion of control that Hacktivismo's projects enable.

This subversion of control and power works at both functional and symbolic levels. At the functional level, Hacktivismo's projects – their software-based counterpublicity – serve to 'hack out' spaces of discursive freedom within which Internet-based counterpublics can be instantiated. The citizens of repressive regimes can use software tools such as Torpark and ScatterChat to escape the control of their governments, and construct their own counterpublics within what is otherwise a totally controlled arena. They can escape (at least partially) from the national pseudopublics they are forced to conform to, accessing information and discourses, political and otherwise, from a wider global modular network of publics and counterpublics, using these spaces to solidify their own counterdiscourses and, if they wish, construct their own externally-oriented counterpublics that are critical of and work against the overarching and repressive pseudopublics that seek to claim them as acquiescent members. They can subvert the control of their governing pseudopublics from within, inserting themselves within these spheres with the effect of placing internal pressure upon them and thus effecting cracks or fractures in their façade.

If extend this counterpublicity and fracturing of hegemony into the global domain, moving from having an internal orientation to an outwards orientation, they can convey their oppositional counterpublicity to the wider global modular network of publics, in the hope of informing and conversing with these global citizens and gaining sympathy for their plight. Ideally, at least some of these global citizens will consequently form their own sympathetic counterpublics, linked by chains of discursive equivalence to those of these repressed but actively oppositional citizens. In this way, the pressure of combined or linked counterpublicity may be brought to bear on the repressive regimes from both inside and outside their nation states, as well as upon the Western governments and corporations who are complicit in their activities.

Again, the recent case of the repression and online dissent in Iran, which garnered a wider global audience and condemnation of the government's activities, provides an identifiable instance[34] of this subversion of pseudopublic control and enabling of multiple and linked counterpublicity. This kind of modular networked counterpublicity serves to not only undermine the authority of these explicitly repressive regimes, but also the corporations and more subtly repressive Western states that either facilitate explicit state-political repression or stand idly by and allow it to occur or continue, while displaying a more democratic façade. The multivalent counterpublicity hopefully enabled by Hacktivismo's software thus works to threaten multiple levels of dominance, mounting a multi-pronged challenge to the political-economic hegemony they oppose.

Hacktivismo's counterpublicity is thus both functional and symbolic, undermining both the appearance and actuality of hegemonic control and uniformity that this public of pseudopublics works to project. Hacktivismo's programmes threaten what discourse analysts describe as the 'face' (Brown & Levinson 1987, following

[34] It is extremely difficult to track what actual effects Hacktivismo's software has had in terms of allowing repressed national citizens to construct both internally oriented and externally oriented counterpublics. Certainly, as previously stated, Hacktivismo have received communication from users thanking them for their products, so they are presumably being used to construct these internally oriented counterpublics – Tor related technologies, in particular, are known to be in common use. However, it is generally too difficult to track how exactly various expressions of dissenting counterpublicity are emerging from such states as China and Iran, i.e. what software tools are being used to achieve this. The recent situation in Iran was somewhat different, in that the much-hyped Twitter was involved; hence there is some knowledge of the specific means by which dissent was disseminated. As such, it serves as a useful concrete example, in the absence of any identifiable examples stemming from Hacktivismo's projects.

Goffman 1967) of these repressive regimes. Face is defined as "the public self-image that every member wants to claim for himself", and is "emotionally invested, and [it] can be lost, maintained, or enhanced, and must be constantly attended to in interaction" (Brown & Levinson, 1987: 321- 22). The concept of 'losing face', as is the case in its general usage, involves being embarrassed or humiliated. Brown and Levinson go further, in defining two sub-types of face, and two attendant types of face-threatening acts or FTAs:

> **negative face**: the want of every 'competent adult member' that his actions be unimpeded by others;
>
> **positive face**: the want of every member that his wants be desirable to at least some others.
>
> (Brown & Levinson 1987: 322; bold in original)

The speaker in any given situation is generally defined as S, and the addressee as H, and the face of both may potentially be threatened or undermined by S's discourse. Interactants are generally considered to be individual speakers, but as should be obvious, the concept of face works just as well for the ideologies discursively expressed by and constitutive of public spheres. In the case of hacktivism, the hacktivists are clearly identifiable as S, and we are therefore concerned with the threats made to H's face through hacktivist counterpublicity, with H consisting of the targets or dominant publics the hacktivists are attempting to destabilise. Acts that threaten H's 'negative-face want' "[indicate] (potentially) that the speaker (S) does not intend to avoid impeding H's freedom of action", and include such acts as orders, threats, the unwanted incurring of debt, and expressions of envy or anger. Acts that threaten H's 'positive-face want' "[indicate] (potentially) that the speaker does not care about the addressee's feelings, wants, etc.", and include such acts as criticism, disagreement, the expression of violent emotion, the raising of divisive topics, and non-cooperation (ibid.: 324-25).

However, as Brown and Levinson note, "there is an overlap in this classification of FTAs, because some FTAs intrinsically threaten both negative and positive face (e.g. complaints, interruptions, threats, strong expressions of emotion, requests for personal information)" (ibid.: 325). This overlap "clearly raises certain problems" and "[calls] into question whether such a clear distinction between positive and negative face is, in fact, a useful one" (Harris 2001: 463; see also Hernandez-Flores 1999; Mao 1994). As Harris goes on to state, "there are undoubtedly many discourse contexts, including much casual conversation, where positive and negative politeness strategies are very likely to co-occur" (ibid.). Hacktivism, which often combines threats to H's negative face, such as putting pressure on H to do something (or cease doing something) through requests, threats and warnings, and through expressing strong negative emotions that exhibit motivation for harming H or H's goods; and threats to H's positive face, such as criticism, accusations, challenges, irreverence, non-cooperation and the raising of divisive topics, is clearly such a discourse context or genre. As such, becoming enmeshed in exactly what aspect of H's face is being threatened by any given instance of hacktivism is counter-productive – the important point is that either through discursive content or form, or some combination of the two, hacktivism mounts a threat to the face of the dominant publics it engages with, in an attempt to provoke political preference reflection and destabilise these dominant discourses.

Hacktivismo's projects clearly and intentionally threaten the overall face of the pseudopublics of repressive regimes; indeed, they break the repressive national laws of these regimes, showing them to be both reprehensible and impotent. Rather than writing a letter to Beijing, or signing a petition against Internet censorship, or any of the other usual and often ineffectual modes of communicative dissent against authoritarian regimes, they directly challenge their control and power by showing that their dominance can be undermined or bypassed, through enabling blatant non co-operation with their desire for control. In doing so, they simultaneous criticise, express anger about, and exhibit disapproval of the operations of these regimes, as well as the Western governments and corporations that are complicit in their operations, by allowing dissident citizens within them to access and engage in taboo or divisive discourses. Beyond this, Hacktivismo's counterpublicity, and the dissident citizen counterpublicity their projects enable, also amplifies their critiques

by being simultaneously directed towards a wider global public of publics, with the intent of generating yet another level of sympathetic counterpublicity within this global arena.

The subversion of legally mandated control and repression, that is, the transgressive nature of Hacktivismo's counterpublicity, serves to propel their actions and their attached constitutive ideology, as expressed in the Hacktivismo Declaration and the press releases and other media statements that paraphrase it, into the global media. These media, in line with Habermas's description of the refeudalisation of society and of the public sphere (1989), may also be considered to be a pseudopublic, in that they generally ignore topics and discourses not relevant to their elite governmental and corporatist motives and maintenance of power, and enable primarily the consumption of, rather than participation in politics. However, the form of Hacktivismo's hacktivism, like much successful activism, creates a spectacle, providing these media with a novel source of news, and thus enables Hacktivismo's counterpublicity to 'hack' its way into the media pseudopublic. As Downey and Fenton remind us, successful counterpublicity relies upon this kind of effective interaction with or use of the mainstream media (2003: 193), in order that they may "actively and effectively contest the discursive boundaries of the mainstream public sphere" (Dahlberg 2007a: 57). By bringing these issues into focus, and bringing concerns from the periphery of the mainstream public sphere and towards the centre, "the structures that actually support the authority of a critically engaged public begin to vibrate. The balance of power between civil society and the political system then shifts" (Habermas 1996: 379), thus creating the possibility of hegemonic fracturing or destabilisation.

The public counterpublicity or impoliteness Hacktivismo direct towards the public of pseudopublics they oppose through the form of their hacktivism (that is, with their software) is further amplified by the face-threatening challenges and negative characterisation inherent in their Declaration. The discursive content of their hacktivist counterpublicity (including the extensive discursive work they do to establish their authority and authenticity) is propelled into the global media public by the transgressive form of their software. The media coverage of their projects in various influential online technews publications (such as Wired, BoingBoing and

The Register), as well as more mainstream news sites (such as the BBC and Bloomberg Businessweek), and the fact that Oxblood Ruffin has written and continues to write articles for assorted influential online 'technews' publications (including BoingBoing, The Register, and Techradar) is testament to their "effective counterpublic strategizing" (Downey & Fenton 2003: 193), as the cDc 'In the Press – Publications' page of their website shows.

This propulsion of discursive content into the mainstream through form generates multiple levels of agglomerative counterpublicity, not only censoring explicitly repressive regimes, but also the technology corporations that do work for these regimes and the hypocritical Western democracies that decry internet censorship while implicitly sanctioning it through welcoming the profit it generates, and sometimes even engaging in internet censorship themselves. The operations of this public of pseudopublics are exposed as fallible, and their positive face is threatened through both the form and content of Hacktivismo's counterpublicity.

The inherent counterpublicity of Hacktivismo, and the consequent levels of counterpublicity they enable, is a purposive attempt to embarrass and humiliate these pseudopublics, with their purposive and politically charged impoliteness clearly intended as a form of counterpublicity oriented towards the destabilisation of political-economic hegemony. Furthermore, Hacktivismo's counterpublicity creates cracks and fractures within which further counterpublicity can flourish. The counterpublic sphere constituted by Hacktivismo's embedding of their ideology within code is not only counterpublic in and of itself, but it also intended to be a catalyst for a further cascade of viral counterpublicity, through the provocation and hopefully alteration of political preference, generating a wave of dissident communication and counterpublics that are all ultimately oriented towards the destabilisation of the dominant publics and ideologies that they oppose.

7.4 Summary of Hacktivismo as a counterpublic

We can thus see that both the discursive form and the discursive context of Hacktivismo's counterpublicity work in combination, constructing Hacktivismo's external counterpublicity, which attempts to both provoke political preference reflection and to destabilise the relevant dominant publics they intend to counter. The Declaration serves to legitimate Hacktivismo and their ideology as worthy of support, and to define and critique the dominant publics and the reprehensible behaviour against which they are oriented as counter. Their software projects embody this critique and dissent, and propel it into a wider realm of publicity, thus amplifying the strength of Hacktivismo's counterpublicity as a whole. Their hacktivism's potent combination of form and content, grounded in a multivalent subversion and manipulation of various hierarchies of communicative power and access, is what constructs both the basis and strength of their counterpublicity. This powerful combination of content and form is a defining feature of hacktivist counterpublics engaging in successful (that is, visible) external publicity, as is further demonstrated in the following two case studies.

Chapter 8

Performative hacktivism: The Creative Freedom Foundation and the New Zealand Internet Blackout campaign[35]

8.1 Context

The Creative Freedom Foundation are a group of artist-activists (Samuel 2004a) founded in 2008 by New Zealand artists and technologists Bronwyn Holloway-Smith and Matthew Holloway, in response to proposed changes to New Zealand (NZ) copyright legislation and out of concern for the damage these changes might wreak upon the creativity of the NZ arts scene, the economy, and public rights[36]. These founders, and a third trustee, Luke Rowell, spearhead a diverse collective of NZ artists, including musicians, filmmakers, visual artists, designers, writers and performers, and are additionally backed by the support of thousands of NZ citizens, forming an extensive nationally-based counterpublic. In terms of keeping the organisation alive, they are supported by "a network of members who often volunteer their time and skills to help with different aspects of the CFF" (Holloway-Smith 2009).

The CFF's work is ongoing – they are currently involved in the NZ and international coalition aimed at opening up the ACTA negotiations and rendering the formation process of the legislation democratically accountable – but their original catalyst for formation was the proposal of the so-called 'Section 92'[37] Amendment to the NZ Copyright (New Technologies) Amendment Act (CAA),

[35] In line with the principles of critical discourse analysis and disclosure in general, the author would like to state that she is a supporter or member of the Creative Freedom Foundation, and took part in the Internet Blackout.

[36] As in the previous case, much of the information on the CFF is taken from their website, and as such, inline citations will only appear when direct quotes or specific pieces of information from their site are used. Inline citations will, obviously, be used as normal for all other sources.

[37] The contentious sections are actually S92A and S92C, not S92B or C, or any of the other subsections, but the shortened reference S92 is in common use in NZ, and will be used here for brevity.

which was passed in parliament in 2008 and was intended to come into effect on the 28th of February, 2009.

8.1.1 Section 92A and C of the NZ Copyright Amendment Act

This Act would have implemented a 'graduated response' or 'three-strikes' approach aimed at countering copyright infringement. This approach takes various forms, but is based upon the premise that three accusations of copyright infringement will lead to the termination of the accused's Internet connection by their relevant ISP. In the case of the CAA, these accusations were not required to be supported by legal proof, thus legalising termination without the need for a trial or for evidence to be held up to scrutiny in court. This led to the amendments being described by many (including the Creative Freedom Foundation) as the 'Guilt Upon Accusation' laws, and indeed, the amendments rendered the legislation "arguably the world's harshest copyright enforcement law" (Saarinen 2009). As explained by one of New Zealand's leading media and political bloggers:

> It is not only that this law denies the accused any due process, it is that **it stipulates a penalty that no court would impose in adjudicating a copyright complaint** even if infringement were proven. Remarkably, someone convicted in a court of law of handling child pornography via the internet would not suffer such a penalty.
>
> (Brown 2009a; emphasis in original)

The amendments would have also changed the definition of an Internet service provider (ISP) to become "practically anyone with a shared connection or website" ('Join the Internet Blackout'), thus rendering businesses, schools, libraries, governmental departments and many other organisations and individuals ISPs, and

as such, responsible for logging all connections under their purview in order to provide evidence for possible accusations of infringement. This provoked widespread ire, with libraries voicing particularly strong opposition, as the logging requirement "practically expects your organisation to know both data forensics and copyright law" (ibid.) – an instance of massive and inappropriate burden shifting from copyrights holders onto any entity providing Internet access.

The 'three strikes' approach is one of the mechanisms being lobbied for by the entertainment industries in their efforts to reinforce copyright legislation by imposing ever-harsher penalties on infringers. In New Zealand, the Recording Industry Association (RIANZ) actually rejected a draft code of practice for ISPs written by the Telecommunication Carriers Forum that sought to neutralise some of the worst aspects of the new amendments as inadequate, stating that it made it too easy for those accused to dispute allegations of piracy (rather than just being guilty upon accusation), and did not go far enough towards protecting copyrights holders' interests (Saarinenen 2009; Pullar-Strecker 2009).

Business funded-studies carried out by the entertainment industry regularly claim massive losses due to 'piracy', such as the Microsoft-backed lobbying group the Business Software Alliance's 2007 'Piracy Study' claiming revenue losses of US$29 billion due to pirated software (BSA 2007). Indeed, these claims have been remarkably successful in terms of attaining discursive dominance, with the idea that 'piracy is killing the film/music industry' being frequently and unquestioningly mobilised within mass mediated public spheres. This is hardly surprising, given the heavily concentrated and conglomerated status of the global media sector, with music and film studies economically interlinked with the news media and sharing the same ideologies and motivations. However, there is arguably little actual evidence to support these claims of industry annihilation, which form the basis of rights holders' rationales for ever-tighter copyright legislation, in order to 'protect artists' (such as musicians and film makers, rather than the actual production labels and corporate rights holders). A recent study by the United States Government Accountability Office dismissed many of them as being based on unreliable methods, and some industry bodies, including the MPAA, refused to divulge the details of their methodologies and calculations at all (USGAO 2009). The fact that

media corporations such as Sony continue to have 'record-breaking years' in terms of box office returns casts further suspicion on industry claims of being crippled by Internet piracy (Masnick 2009), and it is arguable that their coining of the 'piracy discourse' is evidence of a sluggish and conservative corporate mindset that is unwilling to adapt (and invest in adapting to) new technological environments and modes of content delivery.

The '3 strikes' approach is intended to complement these media conglomerates' ongoing litigious strategy of suing copyright-infringing websites (such as Napster, and more recently, The Pirate Bay) and individuals, and pushing for national adoptions of supranational legislation such as the World Intellectual Property Organizations (WIPO) treaties and the Anti-Counterfeiting Trade Agreement. (ACTA). This international pressure to adopt such legislation domestically is driven by a neoliberal free trade agenda, with smaller nations allegedly being held to ransom by global powers, primarily the United States. The CFF's suspicion with regards to the drafting of S92, as described by one of their core members, is that the NZ government, like many others, was "concerned about New Zealand having signed various WIPO treaties and that the country might not get a free trade deal with the US unless the entertainment industry that vigorously lobbies the US Trade Representative gets its way", thus NZ sovereignty was going to be "sold down the river" on the sly (Saarinen 2009).

8.1.2 The Creative Freedom Foundation

The CFF counterpublic was founded in late 2008 in response to the impending amendments. As Holloway-Smith described:

> As an artist I was concerned that those claiming to represent artists didn't represent how I felt about the issue, and after conversations with other artists friends of mine who were equally concerned I quickly

> became aware that there was need for independent artist representation on the issue.
>
> (Holloway-Smith 2009)

They created a website, around which they constructed a core activist counterpublic, compromised of NZ artists, technologists, and other interested citizens, primarily through:

> …already established relationships. Some new ones emerged through mutual friendships and also through email contact.
>
> (Holloway-Smith 2009)

The CFF's primary and ongoing goals are to "encourage[s] and facilitate[s] discussion, provide[s] education, and seek[s] to answer emerging questions around issues that have the potential to influence New Zealand artists' creativity" (CFF). They also endeavour to act as advocates for artists' views on these issues, and to foster a healthy, vibrant NZ arts community, and through these goals, "seek to bring Copyright Law into the 21st Century" (ibid.). Their three main legislative concerns about which they aim to "spread the word" ('Section 92') are S92 (which they variously describe as the 'Internet Termination Law' and 'Guilt Upon Accusation Law'), Digital Rights Management ('DRM Free NZ'), and legislatively mandated Internet surveillance ('No companies snooping on your Internet'), although we will focus exclusively on their first goal and the associated campaign in this analysis.

They keep a 'featured' article by Nat Torkington, a NZ computer programmer and author, and their friend and co-member, in a fixed position at the top of their website's page directory, with this article articulating the base of their counterpublic's 'intellectual ideology', which is structured around their views on the Internet and current trends in copyright legislation. They regard the Internet as a

boon for artists, in that it provides "new opportunities to reach fans and new opportunities to earn a living", and see the corporate media intermediaries pushing for increasingly punitive and restrictive Internet-related copyright legislation as "not safeguarding [artists'] interests" (Torkington 2008). Rather, they see these proposed legislative changes as "fight[ing] progress" and "alienating fans rather than figuring out how to turn them into satisfied customers" (ibid.).

Figure 7: The Creative Freedom Foundation's logo[38]

8.1.3 The CFF's intellectual ideology

The website is thus the space in which the CFF discursively generate and maintain the base of their counterpublic, which includes explicitly articulating their overall

[38] Image from: http://creativefreedom.org.nz/library/creative-freedom-logo/logo.png

intellectual ideology (Billig et al 1988), and their specific intellectual ideology regarding S92. They do much discursive work to characterise the impending legislation as exceedingly negative, by both establishing the importance of the Internet to everyday life and to human creativity, and articulating how the legislation will both erode the positive functions of the Internet, as well as contravene citizens' rights to a fair trial, amongst other violations. This discourse, by extension, characterises them as defenders of both Internet and citizen freedom.

They are positive about the potential for technology to enable human progress, articulating their belief that "[i]n future years, the internet will continue to become more pervasive", and outline its importance for easing the temporal and geographical burden of everyday activities such as banking, bill paying, education, and interpersonal communication ('CFF's Submission'). They also see the Internet as "part of modern free speech", and this, combined the with previously mentioned moving of essential services and utilities online, means that legislating terminating citizens' Internet access is "too severe a punishment" and will only become 'increasingly unfair" (ibid.). As such, copyright legislation must be "updated for the modern age", and they argue that implementing S92 will only necessitate "revisiting a law that will be outdated in the near future" (ibid.).

Indeed, they see Internet access as a basic human right, and "have grave concerns with recent trends in international copyright laws that bypass the traditional expectations of civil rights (such as due process)" ('Section 92'). They describe S92 as legislation that "forces the termination of internet connections and websites without evidence, without a fair trial, and without punishment for any false accusations of copyright infringement", with public rights "drastically undermined by a law that automatically treats people as criminals" ('What is copyright?'). They repeatedly describe the legislation in extremely negative terms, using strong adjectives such as disproportionate, "too severe", "unfair" ('CFFs submission'), "unjust", "ripe for abuse", and "dangerous" ('Section 92'), and point out that similar overseas laws have been "used to limit free speech", providing links to examples of this occurrence ('Section 92').

They also see the Internet as a space for creativity, artistic endeavour and direct connections with fans, as well as community building, with these aspects being

particularly important for NZ as a geographically isolated nation, describing the Internet as "increasingly becoming the primary way we engage with the rest of the world" ('Join the Internet Blackout'). They regard the current restrictive state of copyright law as restricting this creativity, by criminalising "[r]emixes, mashups, and digital citations [which] are valuable creative contributions to society" ('How Copyright Is Harming Creativity'), and they underline their support for remix culture and creative freedom and sharing in the tools they use, with all content on their website licensed under a Creative Commons Attribution Share-Alike 3.0 NZ License, thus enabling free copying and remixing.

The CFF see S92, specifically, as illegitimate in that it claims to be for the benefit of artists, when the opposite is true, and use the phrase or meme "Not In My Name" throughout their discourse, to distance themselves from the harmful legislation and underscore the dishonesty of its rationale. They repeatedly state that they do not want it pushed through "in the name of artists and protecting creativity" ('Section 92'), and explicitly support 'fair dealing' or 'fair use' copyrights ('What is copyright?'), condemning the legal protection of Digital Restrictions/Rights Management that removes rights citizens would otherwise have ('DRM Free').

They are at pains to point out that "Copyright infringement is wrong" ('Section 92'), and that they do not "endorse or support copyright infringement that takes money away from artists, but instead [we] advocate Copyright reform for the benefit of New Zealand" ('What is Copyright?'), thus establishing themselves as reasonable, and located on the right side of the law. It is the poor form of the legislation that they are opposed to, not combating copyright infringement *per se*. They see legislation such as S92 as evidence of an entertainment industry that is slow or unwilling to adapt to a new environment, but believe that the onus is on them to do so, rather than trying to mould the Internet to suit their purposes, and do not believe that such "unworkable" industry models should be supported by "government intervention" ('CFF's submission'). They quote Telecommunications Carriers Forum chief executive Ralph Chivers, supporting his description of governmental officials as being "technologically uneducated", and being "taken for a ride by lobbyists putting their interests ahead of the nation" ('Section 92').

Indeed, they believe that S92 will actively "harm" ('Our Goals') and "stifle" ('What is Copyright?') creativity, in that "[a]rtists are already using the Internet effectively" ('CFF's Submission') and the legislation will undermine their efforts by "simply pushing illegal downloading further underground" ('Section 92') and provoking a public backlash against artists that will "make it even more difficult to educate the public and convince lawmakers of the necessity of sensible laws to protect creators rights" (Australasian Performing Right Association member, Anthony Milas in 'Join the Internet Blackout'). They see it as "corrosive to the public trust in copyright education that the artists benefit from", and believe it "risks undoing the social contract that underlies copyright", thus "encouraging illegal downloads and taking money away from the creative sector", as well as potentially undermining NZ's connection with the global creative community (ibid.). Essentially, they see S92 as wholly counterproductive, and believe it will actually exacerbate the problems it is intended to combat.

The CFF also emphasise the importance of subjecting the Internet to principles of democratic governance, calling for the defence of civil liberties in digital environments and greater public participation in legislature building, as opposed to the imposition of legislation like S92 from on high, with little to no public consultation. They repeatedly refer to democratic and human rights-based tenets, such as the presumption of innocence until proven guilty, the right to a fair trial, and the right to freedom of expression, all of which they describe S92 as contravening. They present themselves as defenders of these democratic principles, and actively promote increased citizen participation in political decision-making, asserting to their wider counterpublic that "[w]e should speak out about injustices like *Guilt Upon Accusation*" ('Section 92'; italics in the original).

They use hyperlinks to direct citizens to additional information, including online copies of the pertinent legislation, as well as contact information for relevant parliamentary representatives and tips on how to write an effective letter, urging citizens to "keep it polite and respectful, but firm - it's more persuasive that way" ('Join the Internet Blackout'). They emphasize the need for politicians to notice that citizens care about the law, urging New Zealanders to "[s]tand up and make [their] voice heard: Say NO to Guilt Upon Accusation laws" ('Section 92'). Their

focus is not on "pointing the finger at MPs", but is rather on communicating their dissent and thus influencing them to "stop this unjust law" before it comes into effect ('Section 92').

8.1.4 The functions of the CFF website

The CFF are, primarily, an activist organisation, and as such, their website aims to facilitate the wide dissemination of relevant information in a concise and timely manner; enable the discursive creation and maintenance of a wider activist counterpublic, and lower participation thresholds by providing ideas, outlets and tools for their members. Different Internet technologies are used for supporting these activities, with the CFF website acting as an organisational hub for these various applications and uses. They exploit the different communicative functions of web spaces identified by Stein (2009), using various web applications to provide information, promote interaction and dialogue, assist action and mobilization, make lateral linkages, serve as outlets for creative expression, and generate further resources for campaigns (ibid.: 752-753).

The website functions as an alternative media site, providing background on the CFF and their work, as well as regular updates on progress, successes, and new concerns, such as the recent ACTA negotiations. The information they provide strives to be clear and concise, attempting to decode somewhat impenetrable legislation into easily understood points, and explain why their cause is relevant to businesses and organisations who would be classed as ISPs, and artists and individuals ('Join the Internet Blackout') – making their intellectual ideology more accessible to readers and prospective counterpublic members.

The website also provides a plethora of ways in which members of the counterpublic may keep up to date with the latest CFF news – one may subscribe to weekly newsletters; follow links to the CFF Twitter stream, CFF Facebook group, or CFF YouTube channel, or become the CFF's MySpace friend. These latter social

networking technologies provide the added benefit of interactivity – counterpublic members can communicate with one another and with the core leaders of the counterpublic – something that is further supported by the website's contact form and forums. These different elements and technologies help build and maintain the internally oriented elements of the CFF counterpublic, by keeping individuals in touch with one another and promoting and enabling deliberation. Dialogue amongst CFF members is enabled and encouraged, building internal self-definition and solidarity, and refining their intellectual ideology or internal counterpublicity, as is communication with or towards the dominant publics that constitute their adversaries and targets (through such channels as suggesting that members of the CFF counterpublic write emails to the relevant members of parliament involved with the drafting and implementation of the law).

As such, the CFF counterpublic clearly exhibited the internal and external functions described by Downey (2007: 117) from the outset of their formation. It also exhibits the benefits of diverse membership and incomplete internal reification discussed by Fraser (1992), with their intellectual ideology constantly being 'fine-tuned', rearticulated and expanded through the intra-member discussion facilitated by the website and other web technologies. This ongoing process serves to flatten the hierarchy of the group somewhat, and also promotes the maintenance of familiarity and group solidarity. Their external communication (by way of letters to members of government, etc) further promotes solidarity-generation, and also serves to circumvent the potential counterpublic cyberbalkanization that Habermas warns of (2006). Their engagement with dominant publics constructs the state of interpublicity (the presence of discourse across lines of difference) that Calhoun (1997) sees as vitally important in that it connects otherwise disparate and distant publics and counterpublics into a multi-directional and dynamic modular network of public dialogue and deliberation.

However, in late February 2009, the CFF went a step further, amplying this external counterpublicity and deviating from the usual traditional channels of discursive dissent through engaging in an ingenious instance of performative hacktivism. This amplified counterpublicity took a somewhat hybrid form, in that it straddled the border between hacktivism and traditional activism. This intensification of their

external counterpublicity - the NZ Internet Blackout (henceforth, the Blackout) - should be understood as a discrete mobilisational moment in the ongoing external orientation of the CFF counterpublic, but it was the event that most successfully enabled the far-reaching externalisation of the CFF's counterpublicity, thus provoking widespread political preference reflection, and bringing destabilizing pressure to bear upon their adversaries in an attempt to fracture the hegemony of these dominant publics.

8.1.5 The NZ Internet Blackout

The idea for the Blackout stemmed from the 2009 Kiwi Foo Camp (13-15 February) (Torkington 2009), a yearly unstructured gathering or 'unconference' organised and attended by NZ media and technology industry people and policy makers (including the CFF founders), with many attendees being CFF members. (However, it should be noted that the wider blackout form was not conceived at the Camp. It has been used previously; by the Coalition to Stop Net Censorship against the Communications Decency Act, and by the EuroLinux coalition against the directive for computer-implemented innovations generally referred to as the 'Software Patents Directive', amongst others.) S92 was a main theme at the 2009 Camp, and led to the idea for and initiation of the Blackout aimed at opposing it, which commenced as the Camp finished. The existing core members of the CFF counterpublic began 'blacking out' their Internet avatars (profile images) on social media platforms such as Facebook and YouTube, as well as on a range of websites and blogs, stating that they were doing so in support of the CFF's wider campaign against the 'Guilt Upon Accusation' laws.

As technology and media experts and artists, many of these individuals were highly connected online, with large numbers of readers, followers and friends, and the Blackout phenomenon consequently spread like wildfire. This was helped in no small part by NZ-based technologist and journalist Juha Saarinen, who asked the British actor, author and renowned lover of new technology, Stephen Fry, to

participate in the campaign via Twitter. Fry was, at the time, the third most popular user of the microblogging site (MacManus 2009), and his ensuing participation was a huge boon to the externalisation of the CFF's counterpublic, bringing it to the attention of a hundreds-of-thousands-strong global audience (see Figure 7 below).

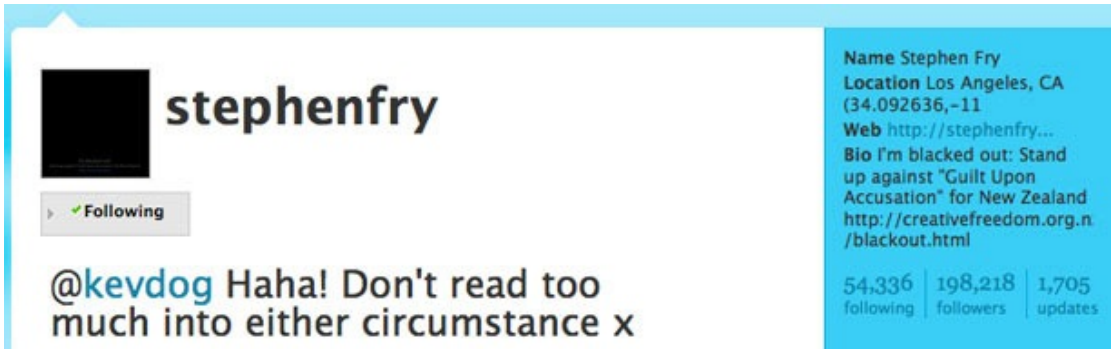

Figure 8: Stephen Fry's blacked out Twitter avatar and Bio referring his followers to the CFF website[39]

By the time the CFF formally announced the Blackout via a press release and through their website and newsletter on February 16, 2009, there were already thousands of participants, and this number continued to grow in a viral fashion. The press release and internal communications directed readers to the CFF website, which, along with the various social media platforms, served to both enable the joining and consolidation of new membership into the CFF counterpublic, and facilitated a viral mobilization of external counterpublicity by disseminating action alerts, coordinating the campaign, and enabling citizen participation.

These modes of participation involved guidelines for traditional activist counterpublicity such as writing emails to pertinent governmental ministers or deputies, signing an online petition (which garnered over 17000 signatures, but is no longer online), and providing details of an offline demonstration to held on the steps of parliament, and of course, how to join the online hacktivist counterpublicity or Blackout. Website and blog owners were provided with instructions and tools for blacking out their sites or displaying banners and logos, with instructions and tools

[39] Image from: http://www.readwriteweb.com/images/stephenfry_twitter.jpg

also supplied for the blacking out of Twitter, Facebook, MySpace and Bebo pages and avatars. Cartoons, a satirical 'copywrong song' remix challenge, and lists of those involved added encouragement, reassurances of solidarity, and the carnivalesque energy often found at offline protests utilising mass involvement and performative or Situationist-inspired tactics.

As a result, for the week spanning February 16-23 2009, the 'lights went out' all over the NZ Internet (Johnson 2009), and in various discrete international locations. The first 6 days of the CFF's weeklong amplification of their counterpublicity primarily involved the blacking out of avatars on the previously mentioned social media platforms, which created a self-replicating cycle of counterpublicity, in that other Facebook and Twitter users would see a blacked out profile, follow the link attached to explain the blacking out to the CFF website, and thus be exposed to the CFF's constitutive intellectual ideology, therefore being provoked into political preference reflection. Many of these readers did not just reflect, but altered their political preferences in response to the information provided on the site, and consequently joined the CFF counterpublic and blacked out their own avatars, resulting in more and more participants.

It is impossible to quantify the number of people who blacked out their various avatars during that week, but they were numerous, as the '#blackout' twitter hashtag during the time showed, and their number included not just Stephen Fry, but several other national and international technology and media opinion leaders, including Cory Doctorow, Leo Laporte, and Neil Gaiman, all well-known figures within the technology and literature community. The CFF kept a partial record of participants in a forum thread on their site, which ran to 120 posts, and each post details at least one, and in most cases, several different participating sites or individuals, thus hinting at the magnitude of the counterpublicity ('Groups/People joining the Internet Blackout').

Figure 9: The CFF Blackout page ('Blackout Homepage')

The last day of the weeklong protest involved blog and website owners redirecting requests for their homepages to a specially constructed page on the CFF website, stating that their page had been "voluntarily blacked out" in protest against the impending S92 legislation (see Figure 8), or placing a blackout banner on their homepage. Some CFF members had been engaging in this activity all week, but the core action took place throughout the first half of this last day. This final, more drastic stage of the Blackout was observed primarily within NZ, with a wide range of websites participating. Blogs from both sides of the political spectrum blacked out their sites, including Kiwiblog, Public Address, Gotcha, The Standard, Not PC, No Minister and Frogblog, all of which are consistently rated amongst the top 10 most popular blogs in the NZ blogosphere ('TUMEKE! NZ blogosphere'). Various members of parliament from both sides of the political spectrum also blacked out their personal blogs. The NZ community news and raw news aggregation website Scoop.co.nz, which garners around 25000 visitors a day (including many journalists looking for story leads) participated ('About Scoop'), as did the "[h]igh profile

mapping service provider" Zoomin.co.nz, which blacked out all its maps, thus symbolically "placing NZ in a perpetual state of virtual darkness" (Pilcher 2009).

8.1.5.1 The Blackout as performative hacktivism

This instance of performative hacktivism (Samuel 2004a) highlights the diversity of forms that hacktivism, and particularly performative hacktivism, can take, as well as the potential for the remixing of different forms, and their combination with more conventional forms of Internet-enabled activism (such as information dissemination, organising offline mobilisation, signing e-petitions and sending emails to members of parliament). The blackout protest form is a hybrid, encompassing elements of both the conventional and disruptive (hacktivist) tactics outlined in Costanza-Chock's matrix of electronic repertoires of contention (2001). It is conventional in that the citizen activists deploying it alter only their own web environment, but disruptive in that if these activists are website or blog owners, and particularly if their sites or blogs receive a lot of traffic, then their readers will be temporarily denied information they have come to expect on an ongoing and regular basis.

In terms of hacktivism's internal typology, it is situated within Samuels' category of performative hacktivism, which is carried out by artist-activists (which the CFF founders and blackout initiators certainly are), and which takes a transgressive form; that is, it challenges the legal and political order but still exists in relation to it (2004a). Akin to Downey and Fenton's description of counterpublicity, it seeks to challenge the status quo rather than escape from it completely (2002). It is a hack in the sense that it is an ingenious and creative use of technology in a manner not originally intended, and its element of illicitness stems from the way in which it breaks the "perceived rules" of blog and websites' information flow (Turkle 1984), and mimics the more transgressive or outlaw forms of virtual sit-ins, defacements and redirects. As such, it borrows from a multitude of different forms of hacktivism, not just those generally found within the category of performative hacktivism.

It uses a (voluntary) website defacement by means of redirection, a form usually utilised by Samuel's category of political crackers (2004a) – indeed, as an article in The Guardian noted, 'despite all appearances', the blackout wasn't "the result of a malicious hacker" (Johnson 2009). This form is amalgamated with what Jordan and Taylor (2004) describe as Mass Action hacktivism's (later subsumed into Samuel's category of performative hacktivism) defiance of "the lack of physicality in online life, in favour of a mass collection of virtual bodies that are not yet present to one another" (ibid.: 69), but which provide the critical mass necessary for the hacktion to succeed. This second element is something that we would generally expect to see in virtual sit-ins, which are one of the main two commonly identified forms of performative hacktivism. However, we may also understand it as utilising elements of the other common form of performative hacktivism – satire, such as that utilised by the Yes Men – in that it is essentially a satirical form of political cracking. The Internet blackout mimics site defacements or redirections, although magnified across a much broader range of sites, yet manages to avoid the illegality of such actions.

As such, the blackout form remixes other forms of hacktivism and online activism in new but complementary ways. It provides what we could call (borrowing from the description of political movements) a "third way" with the existing repertoire of electronic contention (Costanza-Chock 2001), which falls between the disruptive and conventional forms. Only time will tell whether or not it is representative of a new era in performative hacktivism and online activism in general, but given the increasing usage of the blackout form (one was recently used to protest against Internet censorship in Australia); the emergence of such paradoxical and subversive phenomena as a Facebook group dedicated to helping people to delete their Facebook accounts (in protest against the site's recent privacy woes), which at the time of writing had almost 50,000 members ('How to permanently delete your Facebook account'); and the almost endless possibilities the Internet provides for creative expression and satire, one suspects that we have only just begun to see what imaginative forms of online political protest are possible.

8.1.6 The Creative Freedom Foundation's constellation of publics

As in the previous case of Hacktivismo, and as is apparent from their website based discourse, the CFF and their counterpublicity exist in relation to not just one dominant public, but in relation to several, which are aligned behind a primary dominant governmental public, as well as in relation to a wider national and global 'public of publics'.

8.1.6.1 The New Zealand Government and politicians

Clearly, the primary dominant public against which the CFF orient their external counterpublicity is that constituted by the New Zealand Government and politicians, who presume to speak for the citizens of New Zealand through the legislation they draft. This dominant national public, if we are to use Habermas's term, is once more a pseudopublic, in which politics are generally displayed before but not truly and thoroughly participated in by citizens (1989). The now defeated Labour-led Government, headed by Prime Minister Helen Clark, were the ones who initiated the S92 legislative reform, which was supported by all the other NZ political parties apart from the Green Party. Upon their defeat in the 2008 NZ general election, the incoming National-led Government (headed by John Key) continued with the planned installment of the legislation, despite growing opposition from the other political parties, who appeared to gradually come to realise how poorly worded it was. As previously mentioned, this poor wording left its interpretation open to such unnecessarily punitive measures as ignoring the honoured tradition of being 'innocent until proven guilty', removing citizens' Internet access without a fair trial, and placing the onus of implementing the legislation upon a group of very broadly defined ISPs, thus providing copyrights holders with their desired outcomes without them taking any real responsibility (Farrar 2009).

Thus, although the bulk of the NZ political parties (with the exception of the Green Party) originally constituted a broader dominant parliamentary public of publics, the chains of equivalence between them gradually eroded until the National-led Government were the lone dominant public in ultimate control and support of the legislation, with the other parties reorienting themselves as counterpublics (alongside the CFF and various other entities) opposing the legislation. Indeed, members of most of these political parties ultimately joined in the Internet Blackout in some way or another (Apostolou 2009), echoing the involvement of blogs from across the political spectrum. As New Zealand functions under a mixed-member proportional (MMP) parliamentary system, this consolidation of the opposition and coalition parties generated a power bloc of greater magnitude than that of the National Party. As such, National's continued insistence on the passing of the legislation was truly representative or publicity being paraded 'before rather than for the people', as they were completely unable to claim any kind of representative majority.

8.1.6.2 Copyrights holders and international neoliberal institutions

The institutional bodies and corporations of the copyrights holders (such as RIANZ) also constitute a corollary dominant public or publics to the previous Governmental public, as do the more dispersed associated forces of international neoliberal institutions, who are continually agitating for harsher copyright legislation and attempting to force or coerce (through lobbying or free trade agreements) the New Zealand Government to adopt legislation that fits their own corporate political economic agenda. As such, we can interpret the situation as involving some element of push and pull over a central public with the power to enact or block the ideologies of other counterpublics. The NZ Government and politicians, and eventually just the National Party - the dominant public against which the CFF counterpublic was oriented - were and are in fact being simultaneously pressured by the publics of these rights holders and neoliberal institutions. The CFF

counterpublic does not directly target these latter publics, but they are implicitly opposed or dissented against through the CFF's orientation towards blocking the National-led Government from enacting legislation that works in the favour of rights holders and a neoliberal free trade agenda, at the expense of the good of NZ citizens. Again, Keane's (2000) notion of a global modular network of differently sized publics and counterpublics is useful in conceptualising this situation. Although the CFF do not orient themselves directly towards these corporate and institutional publics, they are connected to them by the intermediary public of the New Zealand government, rearticulating the idea that the 'global modular network' of publics is linked by chains of not only equivalence (Laclau & Mouffe 1985) but also of influence and resistance, and that these interconnections and exertions of power can function both directly and indirectly. This indirect opposition is arguably an extremely clever strategy on the part of the CFF – rather than directly tackling one of the immensely powerful yet diffuse primary agents of the refeudalisation of the public sphere (the mass media), they sought instead to maintain the freedom of a specific national enclave from their influence, thus embarking upon a counterhegemonic project of a more manageable size, relative to their resources.

8.1.6.3 The wider national and global public of publics

As in the case of Hacktivismo, and in continuation of Keane's multi-leveled concept, the CFF counterpublic is also oriented towards a wider non-specific public of publics, predominantly national and particularly those in the arts community, but also international when and where possible. They aspire to incite a wider discourse about S92 and similar copyright legislation, and to have more citizens join the debate about their own rights and the rights of all Internet users (and suppliers) who will be affected by this legislation. They seek to not only educate and provoke political preference reflection within these diverse publics, but to hopefully convert some of the citizens they access into supporters of their cause. As with Hacktivismo, the CFF's hacktivist counterpublicity was intended to be not just contestatory but also self-replicating or viral, through provoking not just one stage

or layer of political preference reflection but a self-reinforcing exponential flow, hopefully leading to widespread preference alteration. However, unlike Hacktivismo, they did (and do) want more members for their specific counterpublic, to swell the 'ranks of their disaffection', and thus bring a more powerful discursive strength or counterpublicity to bear on the dominant public they oppose.

We can therefore see that the CFF, as a counterpublic constituted by a general discourse against increasingly harsh and restrictive copyright legislation, and against the S92 Amendment specifically, intended for their Blackout campaign to both threaten the hegemony of the dominant public of the National-led Government and to also catalyse a wave of political preference reflection within a more dispersed and predominantly national (but also possibly global) 'public of publics'. This second goal was in aid of the first, in that the amplification of their counterpublicity would bring more destabilizing pressure to bear on the National-led Government, thus simultaneously destabilizing the forces of neoliberalism simultaneously attempting to sway the governmental public to their will. Their counterpublicity was intended to serve as a buffer to this neoliberal political economic influence, not through direct opposition to the neoliberal institutions themselves, but through pressuring and hopefully fracturing the hegemony of the more readily accessible and local manifestation of this global influence – the New Zealand National government.

8.2 Text

Now that we have clearly identified these publics and goals, we may explore how the CFF counterpublic utilised the Blackout hacktivist form to achieve them. The Cff's website and blog Blackout redirect page (previously shown in Figure 8) is clearly the primary text worthy of closer analysis, as it formed the core of the hacktivist component of the CFF's Blackout campaign – it was their most strongly externalised 'public face', and was the more detailed form or culmination of the associated mass blackout of Internet avatars. The linguistic component from this

text is reproduced below, with reference numbering. As the text was read primarily by the NZ readers of blogs and websites whose NZ owners, as members of the CFF counterpublic, had blacked them out in protest against S92 (as well as by those reading the widespread news coverage of the event), the analysis will follow this form; that is, it will be conducted as if we were one of these readers.

> This Website is Blacked Out
>
> This Saturday, February 28th, Section 92A of the Copyright Act is due to come into force. **(1)**
>
> This website has voluntarily been taken down in protest against this law, which will be used to disconnect New Zealanders from the internet based on accusations of copyright infringement, without a trial and without evidence held up to court scrutiny. **(2)**
>
> May we be very clear, we do not support or condone copyright infringement or illegal downloads. **(3)**
>
> But this blatant disregard towards the basic human right to a fair trial is completely unjust and unworkable and it has the potential to punish New Zealand businesses and individuals where in fact no laws have been broken. **(4)**
>
> Similar laws have been rejected in the EU as being against *"a fair balance between various fundamental rights";* rejected in the UK due to *"impracticalities"*, and rejected in Germany as being *"Unfit for Germany, Unfit for Europe"*. **(5)**
>
> We don't care who voted for the law in the first place. We just want it stopped. We call on the Minister responsible, National's Simon Power, to do the right thing and repeal Section 92A immediately. **(6)**
>
> www.CreativeFreedom.org.nz

As represented in Figure 8, the primary and overwhelmingly noticeable aspect of the text is not linguistic, but of a visually semiotic nature. That is, it is black – the websites using it have been blacked out, or annihilated. The CFF and their counterpublic used this blackness to symbolise a number of things. It is emblematic of the barren wasteland that the Internet may become under repressive regulation,

and represents pre-emptive sorrow or mourning for censored creativity and freedom of expression. The CFF also utilised the 'blackness of the blackout' due to the "'black' theme [being] iconic in New Zealand", and because "with the threat of internet termination there was the idea that New Zealanders' connection with the world could be cut off and hence the 'internet blackout'" (Holloway-Smith 2009). This dark void, so jarringly different from the usual content of most websites and blogs, is used not only to grab our attention, but also to underscore the seriousness of the discursive message overlaid upon it, and to plant the above connotations in our minds.

The title of the message the CFF counterpublic embedded within this sea of blackness seems rather redundant, in that it essentially tells us what we feel we already know, but the passive nature of the sentence (in that no actor is identified) informs us that what we are seeing is not an accident – the blacking out has been done purposefully – but leaves us wondering who has actually done it. As such, they prompt us to cease wondering whether there has been a technical glitch of some kind, and wondering where our expected web content is, and rather, begin wondering who has blacked the page out, and why. After using the blackness – the notable and jarring absence of expected content - to catch our eye, and the title of the message to assure us that what we are seeing is purposive, the CFF then spend the rest of the text answering (to various extents) these questions of 'who?' and 'why?' for us.

The first sentence of the text appears to be a fairly unproblematic material clause, letting us know when and what legislation will be implemented, and signaling to us (through its primary placement) that this legislation is the reason why the page we are looking at is blacked out); however, the CFF's use of the modal "due to" as opposed to "will" signals to us that there is a possibility that the implementation of the legislation may not happen (1). In the context of the rest of the text, this leaves open a reason for protest – if the legislation was definitely going to happen, fighting the inevitable might seem pointless, but if it is only "due to" happen, with its implied question mark, then there is more reason for people to get involved and intervene to prevent this from actually occurring. Furthermore, even though the usage is a relatively common one, the CFF's choice of the word "force" rather than

"implement" or some other more neutral verb carries connotations of violence, arguably indicating that this legislation is not positive or beneficial, but will rather impose something unpleasant or undesired upon us.

The CFF then let us know that the blacking out of the website we are attempting to read is voluntary; that is the owner of the site has done it on purpose, and has not been forced into displaying it (that is, their website has not been defaced by a hacker!) (2). As such, whoever it is that owns the website or blog we are trying to read is immediately involved as part of what we are told is a "protest" action against the law mentioned in the previous sentence. These site or blog owners, who we rely on for information and go to in order to hear about their opinion on matters, feel so strongly about the previously mentioned law that they have disrupted their usual operations, and denied us our usual access to their content, signaling to us that the law must be very bad indeed. The CFF use the remainder of the sentence to confirm this suspicion, making a material and unmodalised statement (conferring facticity and authority) that this law will (not "may, or "might") be used to deprive people of their access to the Internet based only on accusations of copyright infringement, unsupported by any trial or court-verified evidence. Given the common understanding and usage of the meme that everyone has the right to a fair trial, not to mention the fact that we are obviously an Internet user, given that we are reading the text online, this immediately signals to us that this law is severely problematic – it may deny us a mode of access to information that we take for granted, through overriding what we generally understand as due or fair legal process. The fact that the site we are currently reading has been rendered inaccessible by the Blackout serves to underscore this message by illustrating what we might come to expect if the legislation is implemented – that is, we may not be able to access information we rely on and take for granted.

The CFF then signal that the protest is a collective action, supported by a group of people, rather than the blacked out site being a solitary action by the site owner, through the use of the pronoun "we" (3). Furthermore, rather than simply telling us that they are reasonable and law-abiding, in that they "do not support or condone copyright infringement or illegal downloads", they politely seek our consent for making this statement, through the use of "may", thus underlining their reputability

as alluded to through their "very clear" statement of their position on the right side of the law. Furthermore, through their nominalisation of the actions of infringing copyright and downloading content illegally (3), the CFF avoid being specifically accusatory against individuals who have been involved in these activities, and thus avoid explicitly alienating these potential new members of their counterpublic. Indeed, copyright infringers have more reason than most to be concerned about the legislation, although the CFF are careful to express their disapproval of this activity.

Furthermore, it is not the status of these activities as illegal that is their collective concern – they are very clear in their support for them being so. Rather, it is the proposed legislation's methods of seeking to punish such activities, in that it will blatantly disregard such human rights such as that to a fair trial, it is unfair and will not even achieve what it is intended to achieve, and it will potentially punish both New Zealand business and citizens for no reason at all (4). The lack of modality in making the first two points assures us that they are factual, and their verbosity – the law does not just disregard, it "blatantly disregards", and is not merely unjust and unworkable, but completely so – emphasises the negativity of this impeding legislation. The potentiality of the last part of the statement is somewhat cancelled out by the use of the phrase "in fact", and the "New Zealand businesses and individuals" being punished are even further removed from any blame, through the passivisation of the laws being broken – they are kept linguistically distinct from any crime, signifying their actual status as innocent, and making their potential punishment appear even more unfair.

The CFF use the next sentence to introduce intertextual support for their ideology, using quotes from unknown parties involved in critiquing similar laws in Europe and United Kingdom to further underscore the impracticality, unfairness, and unfitness of the legislation, as well as its violation of "various fundamental rights" (5). Although we are not informed as to who these words come from (although they are reproduced and credited within the main website), the CFF use the fact that they are taken from critiques of laws that have already been rejected to provide a sense of protest solidarity – they establish a wider global imagined public of counterpublics opposing this kind of legislation, lending credibility and implicit support to the local protest. The CFF's use of this intertextual component also leads

us to understand that if we want to 'keep up with' Europe and the UK, important global regions that we traditionally look to as centres of sophistication (Europe) as well as being the location of (a large component of) our national origin (the UK), then we should also reject this legislation, as they have. They characterise resistance to such laws as 'normal', therefore failing to resist them would, indeed, be abnormal.

Up until this point, the CFF have been very careful to avoid pointing any fingers at specific individuals or organisations – it is the legislation itself that is problematic, and it has been divorced from the actors drafting and installing it though the use of passive sentence structures. Like Hacktivismo, their counterpublicity is primarily oriented towards a cause, rather than a specific entity – entities or organisations are only implicated to the extent that they are involved with the subject of this cause. The law "will be used" (2) "based on accusations", "without evidence held up" (1) – nowhere is any one actor specifically doing any of these actions. The CFF use the last sentences of the Blackout text to consolidate this reason for this purposive avoidance of naming actors – "we"; that is, the group of people involved in the protest do not actually care who voted for the law, it is the law or cause itself that they are oriented against, thus avoiding any impressions of political partisanship, which might alienate some of their prospective supporters. This strategy could also be argued as attempting an invocation of the menacing spectre of the unnamed 'other' – a rhetorical figure that has a long history, particularly within extremist and radical political discourse (and also conspiracy theory), and which serves to add to the negative and threatening discursive construction of the legislation and its enforcers (whoever they may be).

This use of anonymity, whether interpreted as threatening or not, signals that the CFF purposefully intend to be a counterpublic that spans the traditional political spectrum, thus keeping their doors open to a much larger cohort of possible new members, and not imposing a party loyalty-based political limit on the magnitude of their counterpublicity. They are not interested in identifying who precisely is to blame for the legislation, they "just want it stopped" – and they want someone with the power to do so to step up and take responsibility for making sure this happens (6). In the closing sentence, the individual in the position of taking on this

responsibility is finally named – the National Party's Simon Power (the Minster of Commerce), with the CFF publicly requesting (rather than impolitely ordering him to do anything) that he "do the right thing" – the "right thing" being the immediate repealing of the legislation, which is thus oppositionally characterised as "wrong".

The text ends with a hyperlink to the CFF's website, thus directing readers to further, more detailed information on the issue, and with the CFF's logo, thus definitively establishing the name of the counterpublic involved in the protest action and dissemination of the Blackout message. This logo and name serves as a signature to the message, assuring the reader that it comes from some known provenance, and that more information on its authors can be located if desired. The hyperlink also serves to facilitate an ongoing cycle of counterpublicity, directing readers to the CFF website and providing them with instructions on joining the protest they have just been exposed to, thus hopefully swelling the ranks of the CFF, as will be discussed in more detail in the next section of the analysis. The blackouts of Twitter and Facebook avatars used the same tactic but with less immediately available information, combining the eye-grabbing and symbolic blacking out of taken-for-granted information (in this case, the identities and self-representation that are so essential to these social media platforms) with a hyperlink back to the CFF's website, where the more detailed discursive formation of their counterpublicity and of ways to participate in it were available.

The Blackout text's ongoing focus on negatively characterising the legislation, as opposed to negatively characterising the primary counterpublic against which the CFF are oriented (the National Party) ties in with the discourse throughout the CFF's website, which does exactly the same thing. The CFF counterpublic purposefully avoid strongly and specifically threatening the face of the National Party within the content of their discourse, electing rather to characterise the legislation itself as exceedingly negative, and appealing to the good reason of the National Party (and particularly Minister Simon Power) in asking them to abolish what they view as a poorly constructed, impracticable and thoroughly excessive piece of legislation. This, as previously mentioned, avoids alienating National Party supporters and other right-wing oriented citizens who might take umbrage at 'their'

party or side of the political spectrum being attacked, and thus may not have lent their support to the protest, even though they agreed with it in principle.

The CFF also use this strategy to characterise themselves as eminently reasonable and politically objective, in that they do not muddle their discursively constructed counterpublicity with party bias – instead, they remain impartial and equitable at all times, and only want what is good for all of the citizens of New Zealand, not just those in support of a particular party or left/right political ideology. Through their extremely negative characterisation of S92, they cast their opposition to it in an equally positive light. They characterise themselves as a caring and principled force going into battle for the good of all New Zealanders, not just for a select minority.

8.3 Access and control

However, the form of the CFF's counterpublicity did not echo the politeness apparent in the content of the their discourse. The nature of the blackout, as a disruptive and spectacular form of performative hacktivism that constructed its own online discursive event, served to propel the CFF's counterpublicity into a much wider arena than would have been provided by the usual channels of dissent to governmental activity. The rejection of these usual modes of discursive dissent as insufficient, as well as the discourse carried by the Blackout's form, both served to mount a direct challenge to the power and control of the dominant public, and the other publics attempting to influence it – effecting a powerful attempt at fracturing the hegemonic neoliberal discourse behind the legislation. As in the case of Hacktivismo, the form of the CFF's hacktivism served to subvert the usual patterns of power and access to important channels and kinds of discourse, thus provoking widespread political preference reflection (and alteration), and threatening the face of the dominant publics they were opposed to, all in an attempt at destabilising the National-led government (and the forces of neoliberalism pressuring them through trade agreements and lobbying), and specifically, their implementation of S92.

8.3.1 The usual modes of communicative access regarding impending legislative changes

In representative national democracies, there are clear and mandated ways in which citizens are supposed to engage with their parliamentary representatives, particularly with regards to new instances of proposed legislation. Obviously, the usual way in which one shows disapproval of the actions of one's government is to vote for an alternative party in a general election, in the hope that enough other people will share this voting preference, and thus force the current government out of power and usher a new one (and hopefully the party one prefers) in to power. General elections, while arguably the major way in which citizens of representative democracies register their engagement with and opinion of the political representatives and systems that govern them, are heavily controlled affairs. The planning of elections is in the hands of the government and members of parliament, in terms of when exactly they occur, where and how voting may take place, and who may vote.

Furthermore, the planned discursive agenda and indeed, general form of the election as a communicative event is limited to a restricted and binary kind of expression – citizens may either withdraw or offer their support for parties and members of parliament, and there is no provision for more nuanced and specific forms of discursive assent or dissent to, and deliberation of particular aspects of the representative politics at hand (thus Habermas's accusations of pseudopublicity). Furthermore, the registering of one's political preference through voting is forced to be a solitary affair, largely to protect voters from suffering coercion from other citizens or from party members, although this guaranteed isolation also has the effect of limiting the audience for one's political choices and opinions. Citizens are certainly free to disseminate their preferences as widely as they are able, but unless they possess some kind of privileged platform (generally requiring pre-established political capital or financial resources) that gives them access to the mass media, this dissemination is not likely to be very widespread.

Furthermore, given that elections are generally held several years apart – three years, in the case of NZ – even this limited response is not always timely or appropriate, with regards to particular instances of proposed legislation or governmental activity. As such, alternative channels of dissent to particular proposed articles of legislation or intended forms of governance are left open. Politicians make their contact details available, so that citizens may contact them directly using emails or letters, and in the case of New Zealand, postal charges on mail to members of parliament are waived, thus marginally easing citizens' access to their representatives. Citizens who do contact their representatives directly are generally guaranteed a reply, but this reply is often *pro forma,* and there is little evidence to suggest that a few emails or letters expressing dissent to a particular political plan or piece of legislation have much, if any, impact on the final outcome of a particular direction of governance. Additionally, these communications are generally expected to be constructed using formal, rational language and arguments (which, as discussed in the formation of neo-Habermasian public sphere theory, are differentially-available communicative resources), and these letters are once again a solitary affair, not capable of generating any wider and more visible counterpublicity, in and of themselves.

Citizens may also make submissions to select committees, in certain instances, with these providing citizens with yet another chance to register their opinion on a given piece of legislation or parliamentary inquiry. However, as with general elections, the planning, setting and communicative dimensions of these committees are controlled by the parliament, thus reifying the pre-existing power of formal political representatives and structures of governance. Citizens making submissions to these select committees are once again required to follow the communicative rules of access outlined by parliament, including utilising a specific, formal layout and tone within their submission documents. Indeed, the NZ government provides an entire booklet on how these submissions should be structured and presented so that they are "easily read and understood by members of the committee" ('Making a submission'). Little thought is given to the fact that the strictures of this form (again, privileging formal, rational language and modes of argument) are differentially available to citizens, and citizens are expected to invest considerable time and effort in preparing their submission, without any financial or other

assistance, so that the submission may be 'easily' processed by officials who necessarily have access to rational modes of communication and who are recompensed for their time. Once again, there is no guarantee that this time and effort will be met with any change of governmental plans, and the proceedings of most select committees are given little media attention, thus once more limiting citizens' access to a wider audience.

Citizens may also take the option of organising and circulating petitions against certain pieces of legislation, and submitting these petitions to parliament. If they manage to collect enough signatures, they may even (in the NZ context) force the government to administer a (non-binding) referendum to gauge the wider public opinion on a given matter. However, once again, organising and disseminating petitions requires considerable time and effort on the part of the organisers, and without media attention, the social capital required to effect their wider distribution and support can be very difficult to achieve. Even though the Internet has enabled petitions to be distributed and supported much more easily, they still require public attention if they are to be given any significant support.

Furthermore, all this activity occurs in an environment in which governmental and parliamentary officials, as elite sources relied upon by the news media as regular sources of news, have much greater and indeed regular and institutionalised access to the media, and thus a much wider audience for their discourse, than do dissenting citizens or citizen groups. They have much greater control over what issues acquire media coverage, and of the content of this media coverage, and citizens have few chances to participate in this mediated politics. The mass-mediated pseudopublic of national governmental politics is "the court *before* which public prestige can be displayed, rather than *in* which public critical debate is carried out" (Habermas 1989: 201). Elite commercial forces also have privileged access to this mediated sphere and indeed, to the governmental pseudopublic itself (through lobbying and in terms of media conglomerates, through withholding or manipulating governmental access to and portrayal within the media), thus influencing and corroborating with national and international governmental pseudopublics.

All the while, citizens are relegated to limited and largely powerless channels of political participation (including the consumption of mediated politics disguised as

true participation), and rely on this mediated political pseudopublic to inform them of the political world in which they exist. Thus, citizens rely largely on the combined forces of state and economic elites for information about their political environment, with these elite forces having privileged access to both controlling which topics of discourse are displayed in the mediated political pseudopublic, and how these topics are discursively characterised. The CAA is a case in point, being a piece of legislation clearly influenced by the entertainment industry, and, as is the norm for most media regulation (McChesney 2004b), received very little media coverage before the Internet Blackout campaign (and what little coverage it did receive was certainly only in the NZ media).

8.3.2 Bypassing and manipulating these usual channels of communication

It should be noted that the CFF's Internet Blackout campaign involved elements of all these traditional activities of political participation; the core CFF counterpublic encouraged its wider membership to write letters to members of parliament, to sign an online petition registering their opposition to the installment of S92, and the core members prepared and delivered a submission to the select committee collating public input on the CAA, on behalf of the wider CFF counterpublic. As such – it may be going to far to claim that rational-critical discursive strategies are always inherently pointless and should therefore be completely abandoned. Nonetheless, as Eley (1992) argues, the failings that rational-criticality does exhibit can be ameliorated or even overcome by allowing more disruptive forms of communication into the public sphere, such as civil disobedience (and, of course, hacktivism), as long as we follows Dryzek's advice in ensuring they remain non-violent and non-coercive (200)). The Internet Blackout component of the CFF's counterpublicity employs precisely this complementary or intensifying purpose, serving to amplify the magnitude or mass of these usual channels of communication through generating a much wider level of subscription and utilisation than normal to these conventional modes of counterpublicity, and through generating its own

highly public and non-externally mandated expression of counterpublicity. The CFF used the Blackout to generate this uncontrolled channel of discursive counterpublicity, and in doing so, regained control over all the levels of access to discourse, from planning, to setting, to control of the communicative event, and perhaps most importantly, to the scope of their audience. As such, they enacted Young's defense of the right to not only speak within the public sphere or spheres, but also be heard, as well as embodying her identification of passionate communication and activism as ideal modes of realising this right (2001).

The Internet Blackout, as an instance of hacktivist and counterpublic activity, first served to propel the CFF counterpublic's discourse into a wider national and international public of publics, thus once more providing evidence that hacktivism seems to attain a state of interpublicity, or discourse across lines of difference (Calhoun 1997) – as in the case of Hacktivismo, the form of the CFF's discourse launched its discursive content into a wider circulation. The core members of the CFF counterpublic generated a spectacle (the blacked out avatars), much like many other successful instances of protest and performative hacktivism, and utilised pre-existing Internet based connective platforms (primarily Facebook and Twitter) to effect this spectacle, which looked much like an external hack but was in fact internally and voluntarily generated. The interconnections central to these platforms were used to spread awareness of the protest action, directing an ever-widening audience towards the CFF website, where they were exposed to the CFF's intellectual ideology. This ideology carefully constructed so as to negatively characterise the aspect of the dominant public against which they are oriented (that is, the National-led government's proposed implementation of S92), and to positively self-characterise the CFF counterpublic, through their opposition to the law.

Throughout this discursive self- and other- construction, the CFF were careful to avoid overly demonising the governmental counterpublic, instead thoroughly characterising the proposed legislation as utterly reprehensible and thus calling on the governmental public to exercise their inherent 'good sense' and annul it. This tactfulness and positive self-presentation allowed the CFF counterpublic to avoid alienating any particular part of the political spectrum, and to be taken more

seriously by the audience they subjected to their wider counterpublicity. This audience were thus prompted to reflect on their own political preferences, and, due to the carefully constructed positive self-presentation and negative other-presentation encoded in the website, many of these audience members actually transformed or altered their preferences and elected to become members of the CFF counterpublic as well. As such, the CFF engaged in a project of counterhegemonic publicity which generated a self-perpetuating cycle that transformed interpublicity into preference reflection, into preference alteration, then into additional counterpublic participation, which in turn led to further interpublicity.

The successful creation of this cycle owed much to the CFFs thorough provision of new members with instructions and tools for contributing to the spectacle, with the form of the Blackout and the clear instructions of the CFF website dramatically lowering the barriers for these new members' participation. As these new members proceeded to black out their own avatars, they effected a new cycle of preference reflection and alteration, thus perpetuating the viral transmission of blacked out counterpublicity. The use of Twitter and the novel form of the Blackout to garner the attention of various celebrities and opinion leaders, such as Stephen Fry, allowed this cycle of counterpublicity based on ever-increasing audience access to be massively amplified, and to break its way into not just a national, but a global public of publics, through 'hacking into' the news media. Once more (as in the case of Hacktivismo), the CFF proved the ability for hacktivist counterpublics to be not only be relatively powerful (Downey 2007), but to also attract and utilise the skills or advantages of powerful public figures.

The success and magnitude of the blacking out of avatars directed more and more citizen attention to the final day of website Blackouts, and also garnered news media attention to both the current avatar blackout and impending website blackout in both NZ and overseas. During the week of the protest, the blackout was covered by the UK-based international newspaper and website, The Guardian (Johnson 2009); the popular and influential international technology websites and blogs The Register (Williams 2009), ReadWriteWeb (MacManus 2009) and BoingBoing (Doctorow 2009), The Sydney Morning Herald ('NZ blogs in copyright law blackout demo'); and several times in the New Zealand Herald and Stuff.co.nz

websites (Pilcher 2009, Francis 2009, 'Kiwi websites blackout in net law protest'), which together incorporate all of NZ's main newspapers, as well as (more than once) by both main free-to-air NZ television evening news bulletins (see 'Protesters say copyright law stripping rights', 'Blackout protest over controversial copyright law' as examples). The participation of Stephen Fry was mentioned in much of this media coverage, underlining the importance of the CFF's targeting of his participation (and that of other opinion leaders), and the use of Twitter also tapped into an ongoing media fascination with the platform, described by one reporter as the "news media's Twitterphilia" (Williams 2009). Downey and Fenton's (2002) argument that counterpublicity is oriented towards challenging the status quo rather than completely escaping it and therefore necessitates engagement with the mainstream mediated public sphere once more proves extremely prescient.

Of course, this media attention had the effect of provoking even more widespread political preference reflection, which led to the acquisition of even more members for the CFF counterpublic and participants in the blackout, lending an even wider publicity to the action. The final day of hacktivism constituted by the website and blog blackouts, although transmitting the CFF's intellectual ideology to many more New Zealanders and pointing them to the CFF website was, in the end, largely symbolic – the avatar blackout and knowledge that the website blackout was impending were enough to gain the critical mass of audience attention necessary for the CFF counterpublic to gain effect widespread preference reflection and alteration. The blackout of the websites and blogs primarily fulfilled a promise of hacktivist protest, and underscored the internal solidarity of the CFF's counterpublic, in that site and blog owners were willing to take their content offline and replace it with the blackout page, despite this, in many cases, equating to a loss of 'click-through' advertising revenue. The website blackout was a concise summation of the CFF's intellectual ideology, propelled into wider dissemination by the form of the hacktivism, and representing a statement oriented directly towards Simon Power and the National-led government. All the preceding blackout activities pointed towards this final culmination, generating attention for it as the pinnacle of the hacktivism, although the publicity they received ended up disseminating its core message just as well as it did.

The core members of the CFF, much like the core members of other performative hacktivist groups such as the Electronic Disturbance Theatre and their FloodNet virtual-sit-in tool, ensured the success of their action (which relied upon significant participation levels) through lowering participation barriers by providing citizens and CFF members with all the tools they needed to effect the hacktivist action, and instructions on how and when to use them. In effect, they facilitated what we could think of as 'hacktivism-by-proxy' – the core members were the ones who actually planned, organised and enabled the hacktivist event, but they relied on the participation of a significant mass of citizen hacktivists to make it a success. Although this action was not illegal and did not disrupt the websites of the targeted dominant public or publics (in contrast to virtual sit-in tools such as the FloodNet) it achieved very much the same effect in terms of garnering significant media coverage or 'hacking into the media', thus projecting an amplified counterpublicity towards a dominant public, and gathering a wider audience to their website and provoking political preference reflection through both this new website audience and the media coverage. Its disruptiveness was more akin to the satirical parody websites of the Yes Men, in that the CFF counterpublic creatively utilised their own web spaces to cause discursive disruption and thus publicise their intellectual ideology.

Although the CFF website also encouraged its members to use usual channels of communicative access, such as writing letters or emails to pertinent members of parliament and signing a petition, they massively increased the levels of subscription to and thus force behind these actions, with Minister of Commerce Simon Power's office reportedly being "taken aback by the volume of email on the issue" (Brown 2009a), and the previously mentioned petition garnering thousands of signatures in a relatively short period of time. However, this amplification or flood of the usual channels of access for the presentation of alternative discourse was only made possible by the blackout itself, which generated an entirely new channel of communication, directed at both civil society and at the government. This served to operate as an uncontrolled form of discursive access (from planning to setting to control of the event to audience scope), thus bringing widespread counterpublicity to bear on the dominant public of the National-led government, and also putting more weight behind the CFF's submission to the select committee

(which was backed by the thousands of virtual bodies constituting the CFF counterpublic at large).

8.4 Summary of the CFF and the Internet Blackout

As in the case of Hacktivismo, the form of the CFF's hacktivism propelled its content into a state of viral replication, provoking political preference reflection and alteration via cyclical interpublicity and therefore generating a wave of viral counterpublicity which threatened or fractured the hegemony of the dominant National governmental pseudopublic, and of the neoliberal hegemony informing their legislative proposals. This wave of counterpublicity served to act as an oppositional force or buffer against the powerful neoliberal pseudopublics simultaneously orienting themselves towards the Government, directing a flow of counterpublicity through the governments and towards these rival publics, and thus both identifying and contributing to a modular network of publics (Keane 2000) linked by chains of not only equivalence (Laclau & Mouffe 1985) but also resistance and influence. The CFF used the inventive form of their hacktivism to endow their counterpublic discourse with much more power than the usual channels of discursive dissent and political engagement provide. They simultaneously flooded these usual channels and re-established citizen control over access to political discourse and participation through their creation of an alternative discursive channel which subverted or 'hacked' the usual modes of state and corporate discursive control.

It would perhaps be going too far to assert that the CFF's hacktivist-enhanced counterpublicity was wholly responsible for Prime Minster John Key's announcement on the afternoon of 23 February 2009 (the final day of the blackout) that the implementation of S92A would be delayed until 27 March 2009, and his later announcement on 23 March 2009 that S92 would be scrapped and completely redrafted, given various favourable political opportunity structures, such as the newness of the National government and the fact that they had inherited the S92

legislation from their predecessors. However, the CFF counterpublic certainly saw it (and indeed described it on their website) as a victory ('Section 92A has been Delayed!'), in that they had achieved their cause, with the founders distributing the following message to the wider counterpublic:

> There is a lot of work ahead but I hope everyone involved takes some time out to celebrate this victory. This shows how modern online movements and efforts can result in real world change. We couldn't have done it without you -- we've been amazed and humbled by your support. Thanks everyone!
>
> ('Section 92A has been Delayed!')

At the time of writing, the redrafted Copyright (Infringing File Sharing) Amendment Bill has just passed (23 April 2010) its first reading in the NZ parliament, with across-the-board party support. The Bill still proposes Internet termination as a possible punishment for three instances of copyright infringement, but these three infringements would now have to be proven in a court of law, and the court will be required to take the effects of this termination on the user into account. If termination is established as too severe a punishment, fines capped at NZ$15000 will provide an alternative. The Bill also provides a much more fair definition of ISPs and their responsibilities in cases of infringement.

As of 2010, the CFF continue to be engaged with and foster more traditional forms of activism with regards to this issue, and as previously mentioned, are also heavily involved with coalition (or public of counterpublics) of NZ and international activities opposing the secretive negotiations and content of the ACTA.

Chapter 9

Political cracking: Anonymous and Australian Internet censorship

9.1 Context

As will become clear, answering the question of who or what exactly Anonymous are is a nigh on impossible task. They are not a group in the usually definable sense of the word; more a loose and amorphous collection of anonymous online global citizens, who have banded together in various ways and directions and claimed the collective title of Anonymous for themselves. They are a leaderless collective phenomenon enabled by the networked structures and possibilities for anonymity provided online. Their use of the title also indicates the value and power they place in collective anonymity, which is unsurprising given the illegal or borderline illegal nature of the actions of many of their factions or selective mobilisations. However, given that this case study focuses on a particular instance of hacktivism engaged in by one of the (themselves vaguely defined and difficult to parameterise) factions or mobilisations of this complex group phenomenon, some explanation of Anonymous as an overall entity is required.

9.1.1 Who are Anonymous?

Unlike Hacktivismo or the Creative Freedom Foundation, Anonymous are perhaps best described as a concept or a meme that has been instantiated into an amorphous entity comprised of countless unnamed individuals, who periodically cluster into activist formations, both online and off. That is, they are a loosely networked and extremely flexible counterpublic that periodically and autonomously mobilises into more discrete and specific counterpublic configurations, which are defined by the

discursive struggles they engage in, and through their discursive self-presentation. In terms of their hacktivism, the common thread that binds them together despite their diverse membership and incomplete internal reification (states of being common to many counterpublics, as Fraser (1992) argues) is their opposition to information censorship, and particularly internet censorship. Their communal use of Anonymous as a mass noun stems from the ability and tendency for Internet users posting on forums, image boards, and other Internet sites to make comments and contribute to discussion without registering with their 'real life' identity or with an online persona – thus their contributions are attributed to 'Anonymous'. Obviously, not every person who contributes anonymously online is involved in the entity this case study is focused upon, but it is this widespread ability to participate anonymously in Internet communities and fora that has led to their adoption of the title.

The members of Anonymous are comprised largely of sections of the userbases from Internet imageboards such as 4chan.org and 888chan.org. Imageboards are a type of Internet forum or channel (hence, 'chan'), which revolve around images, with users posting their own and commenting on those of others. Perhaps the most infamous of these boards, and one of the most widely trafficked (Sarno 2008), is the English-language board 4chan.org. The site is home to a wide variety of posting activity, with a number of different sub-boards for different topics, including technology, sport, manga, and pornography, both traditional and hentai (sexually explicit cartoons and animations. The site's '/b/' or 'random' board is perhaps its most notorious, as there are very few posting rules and all content is completely anonymous – it is not a place for those with weak constitutions or who are easily offended:

> [P]eople try to shock, entertain, and coax free porn from each other… Customs on /b/ include posts promising photos of personal degradation in return for certain kinds of porn or other helpful information; sarcastically asking for advice on teen romance; sarcastically asking/telling *anything*; pretending to have insider info or be privy to breaking news; posting image puzzles; and raiding other people's sites… /b/ has no rules; pretty much the only thing guaranteed to get a user

> banned is child porn, and even that gets constantly joked about. Reading /b/ will melt your brain…
>
> (Douglas 2008)

The /b/ or random board is widely credited with spawning some of the most persistent and well-know Internet memes (units of viral cultural information), including the immensely popular phenomenon of 'LOLcats' (which involves overlaying an image of a cat (and now, almost anything, not just cats) with an amusing caption).

4chan and other image boards provide enough material for an entire research project in and of themselves, but the general point is that they are phenomena at the heart of a unique Internet subculture, and have served as the breeding ground for Anonymous. The name or meme of Anonymous is taken in large part from the software structure of these boards, which often encourages and sometimes even enforces anonymous posting and commenting. The anonymity and anarchic nature of these boards have combined to generate what one of their members has described as "the first internet-based superconsciousness" (in Landers 2008):

> Anonymous is a group, in the sense that a flock of birds is a group. How do you know they're a group? Because they're travelling in the same direction. At any given moment, more birds could join, leave, peel off in another direction entirely.
>
> (Anonymous member, in Landers 2008)

This self-characterisation is accurate in identifying the dynamism inherent in the membership structures of Anonymous, and also in the organic, collective identity it conjures – considering the diversity and 'weak ties' between group members, it is quite remarkable how they manage to co-ordinate themselves (or at least subsections of the group at large) into effective and highly synchronized units capable of achieving some fairly sophisticated goals. However, the claim to

'superconsciousness' goes somewhat too far – although it is iconic of the rather grandiose self-presentational discourses many Anonymous spokespeople tend to mobilise. However, given the extremely diverse membership of the group and the fact that there have been several instances of group disagreement and splitting into different factions with regards to specific campaigns, if they are indeed a superconsciousness, they are one suffering from multiple personality disorder, with identities that only intermittently coalesce into a singularity. Nonetheless, despite the technical inaccuracies of the descriptor, the 'hivemind' connotations it conjures up do go some way towards characterising the rather impressive feats of co-ordination and single-mindedness they are capable of exhibiting.

The apparently thousands-strong members of this so-called 'superconsciousness' use imageboards extensively to communicate and organise protest activities, as well as various Internet Relay Chat (IRC) networks and wikis, particularly Encyclopedia Dramatica (Davies 2008). They have also created a website ('Why We Protest'), which focuses primarily on their protest activities against the Church of Scientology, and provides further forums for communication and mobilisation. Here, they provide a self-definition for their collective identity, which stresses the power they perceive themselves to hold in terms of their ubiquity and anonymity, and articulates their belief that their ideas and actions can influence society:

> We are a collection of individuals united by ideas. You likely know Anonymous, although you don't know exactly who we are. We are your brothers and sisters, your parents and children, your superiors and your underlings. We are the concerned citizens standing next to you. Anonymous is everywhere, yet nowhere. Our strength lies in our numbers. Our will as a whole is the combined will of individuals. Our greatest advantage is a knowledge of the fundamentals we share as human beings. This knowledge is a fruit of our anonymity… We are Anonymous. You can be Anonymous, too. Together, we can shape society.
>
> ('Why We Protest')

Anonymous (or at least, various factions of Anonymous) have been involved in numerous instances of disruptive online activity, with the entity as a whole not

exhibiting any clear and unified political agenda. Some of these actions have been little more than malicious trolling (activity and communication in online fora and communities intended to cause emotional upset or derail usual topics of discussion), such as the invasions and disruption of the teenage social networking site Habbo in 2006 and 2007 (Singel 2008), and the 'Youtube Porn Day' on 20 May 2009, in which 4chan users flooded YouTube with pornography disguised as children's videos (Cheng 2009). However, other subsections of Anonymous have been involved with clearly articulated politically motivated counterpublic mobilisations, both offline and hacktivist. As previously mentioned, these have been centrally concerned with the free flow of information online, and indeed, the group as a whole is increasingly known for this techno-political orientation; indeed, if there is one central or universal component of their claimed superconsciousness, it is their collective opposition to the curtailment of digital freedoms.

9.1.1.2 Anonymous, activism, and hacktivism

The most well-known and global of these activities, and of Anonymous's activities overall, is their so-called 'Project Chanology', a protest movement against the Church of Scientology, which Anonymous perceives to be involved in Internet censorship, and see as a dangerous and repressive cult ('Why We Protest'). The movement began after the Church threatened YouTube with litigation based on copyright infringement after a video of actor and Scientologist, Tom Cruise, was leaked onto the website in January 2008, in which he vigorously extolled the virtues of the Church. The video was part of a longer Church production, but they claimed that it had been pirated and edited so as to make it look like a piece of slightly lunatic propaganda. YouTube removed the video from their site in response to the threatened litigation (Vamosi 2008). This prompted Anonymous to declare 'war' on the Church through a video response posted to YouTube on January 21 2008, which was followed by a campaign involving the defacement of various Scientology websites, 'googlebombing' to link Google searches for terms like

"dangerous cult" to the sites as search results, and virtual sit-ins and other forms of flood attacks, all intended to disrupt the Church's online operations. Aside from seeing the Church as a 'dangerous cult' involved in attempted Internet censorship, they also protest against its tax-exempt status, seeing it as an organisation that uses its members for financial gains, under the pretense of being a religious body ('Project Chanology'). Project Chanology was and is ongoing, but moved towards offline protest methods after the first month, with members of Anonymous regularly protesting outside various Scientology centres all over the world, many wearing the Guy Fawkes masks that have become emblematic of the group. Some of these simultaneous global protest dates have gathered up to 8000 protesters in over 50 countries across the world (Ramadge 2008).

They were also involved in a collaboration with the world's largest torrent site, The Pirate Bay, creating the website Anonymous Iran ('Anonymous Iran'), which provided support for Iranians protesting against Mahmoud Ahmadinejad's alleged vote-rigging in the June 2009 Iranian Presidential election. The site gave (and continues to give) these protesters tips on how to conduct online dealings anonymously, how to subvert the Iranian firewall and thus gain access to material banned by the government, how to launch various kinds of online hacktivism against pro-government websites, and also lists the best activist Twitter users (Schachtman 2009). Although the 'Green Movement' uprising appears to have been quashed, the site is still active, providing a forum for dialogue and solidarity between those in Iran and their supporters on the 'outside', as well as tools and information.

Clearly, Anonymous is a many-feathered beast, capable of self-organising its diverse membership into a wide array of hacktivist counterpublics. While these members are better described as hacker-programmers as opposed to artist-activists (Samuel 2004a), they have engaged in a wide range of activities that span both Costanza-Chock's (2001) repertoire of electronic contention and Samuel's hacktivist categories of political coding and political cracking, as well as engaging in traditional offline activism and non-political online mischief-making. The fact that they are hacker-programmers coming together in a large online collective, utilising Mass Action forms of hacktivism such as virtual sit-ins (Jordan & Taylor

2004), which are generally used by performative hacktivists, but maintaining an outlaw orientation and using robust pseudonymity or anonymity, further highlights the permeability of Samuel's (2004a) hacktivist typology. While her matrix of origins and orientations and their related nymity practices appears to hold firm, the other variables of collaborative scope, collaborative size, and hacktivist forms are clearly (as she herself states) much more fluid, and if Anonymous is anything to go by, are only likely to become more so.

Given that it is impossible to cover Anonymous's many actions here, this chapter focuses in on one of their factional mobilisations into a hacktivist counterpublic. This counterpublicity took the form of a campaign against the Australian Labor government, and was in response to governmental plans to censor Australians' Internet access. It included both virtual sit-ins or DDoS attacks, as well as defacements, once again highlighting the permeability of Samuel's typology. For brevity's sake, even though an undetermined faction of Anonymous as a whole effected this mobilisation, they will henceforth continue to be referred to as simply 'Anonymous'.

9.1.2 Australian Internet censorship

Before addressing the nature of Anonymous's counterpublicity against the Australian Labor government's plans for Internet censorship, it is useful to possess a brief understanding of these plans, and the problems with and wider opposition to them.

Australia is the sole Western democratic state on the Reporters Sans Frontières' list of 'Internet Enemies' and 'Countries Under Surveillance' (falling into the latter category) ('Reporters Sans Frontières: Internet'). As their website summarises, **"**[u]nder the guise of fighting child pornography, the government wants to set up a filtering system never before seen in a democracy" (ibid). In 2008, the Federal Labor government, led by Prime Minister Kevin Rudd, announced its plans to

undertake testing with the intent of eventually installing mandatory Internet filtering for all Australians. This filter would be similar to those used in China and Iran, with a governmental 'blacklist' of banned sites being rendered inaccessible to Australian citizens.

The primary legislation involved in this plan is the pre-existing Schedule 5 of the 1992 Broadcasting Services Act, which currently vests the Australian Communications and Media Authority (ACMA) with the power to examine and rule on online materials using the film and video guidelines. If the material is 'refused classification' under these guidelines (RC), and is hosted within Australia, the ACMA can order the material to be taken down. If it is hosted elsewhere, the site is added to a blacklist enacted through ISP-level filters, with ISPs already being required to offer this filtering software to their customers ('BSA 1992 Schedule 5'). In most parts of Australia, possessing (but not selling or distributing) RC material in film, publication or game form is completely legal – only child pornography is (of course) illegal overall (National Classification Code 2005).

However, the proposed new legislation, the existence of which was reaffirmed by Stephen Conroy (the Minister for Broadband, Communications and the Digital Economy and Deputy Leader of the Government in the Senate) on 15 December 2009 ('Measures to improve safety of the internet for families'), would require the mandatory implementation of this blacklist-based filter by all Australian ISPs, thus making accessing RC material online illegal, despite it being legal in offline forms. The blacklist itself is secret, comprised of the sites identified by the ACMA and the UK Internet Watch Foundation blacklist, thus total control over what Internet content Australian citizens are permitted access to would be held by a governmental agency (the ACMA) rather than a court, with no citizen consultation or transparency ('Open Internet').

The scope of the proposed filtering is widespread – as is opposition to it. While the stated primary purposes of the filter is to block access to child pornography and protect children online, the problem is that filtering will extend well beyond these aims:

> … thus creating an obvious potential for overblocking. Subjects such as aborigines, abortion, anorexia, or laws governing the sale of marijuana would all risk being filtered, as would media reports or medically related information on these subjects.
>
> ('Reporters Sans Frontières: Australia')

Furthermore, the website Wikileaks (a site and project that Anonymous have increasingly exhibited ideological solidarity with, as evidenced buy their DDoS attacks against Visa and Mastercard following their involvement with denying Wikileaks monetary donations in 2010) published a 'leaked' copy of the blacklist in March 2009 ('Australian government internet censorship blacklist'). This showed that this 'overblocking' was indeed a problem, with some content on the blacklist not even being RC-rated material:

> …about half of the sites on the list are not related to child porn and include a slew of online poker sites, YouTube links, regular gay and straight porn sites, Wikipedia entries, euthanasia sites, websites of fringe religions such as satanic sites, fetish sites, Christian sites, the website of a tour operator and even a Queensland dentist.
>
> (Moses 2009)

Concerns over the filters' effects upon the Internet architecture and flow of information in general have also been raised, with some trials showing marked bandwidth flow performance and filtering accuracy errors (Jacobs 2008). Other trials that Conroy claimed showed that filtering "can be done with 100 percent accuracy and negligible impact on internet speed" (in Crozier et al 2009) were dismissed as lacking in any proper methodology or representativeness by expert Australian statisticians (Ramli 2009). Furthermore (as has been argued in an independent expert report commissioned by the Howard government as well as a report commissioned by Conroy himself), much of the primary material purportedly targeted by the filter (child pornography) is located on peer-to-peer networks not covered by the filter, and filter circumvention software (similar to that created by

Hacktivismo) means that anyone truly dedicated to accessing such material is likely to be able to find a way to do so, filter or no (Sharp 2010; Moses 2008a).

These issues, as well as more general objections to internet censorship of any kind, have informed widespread national and international opposition to the filter. The US secretary of State, Hillary Clinton, spoke out about Internet censorship in January 2010, stating that it breached the (previously mentioned) UN Universal Declaration on Human Rights (Hall 2010), and the Australian government has been specifically criticised as part of a wider global US diplomatic campaign against Internet censorship (Colgan & Elliott 2010; Sharp 2010). This came shortly after Google expressed similar concerns, labeling the proposal "heavy handed" and stating they believe that "government should not have the right to block information which can inform debate of controversial issues" and that "exposing politically controversial topics for public debate is vital for democracy" (Flynn 2009).

Electronic Frontiers Australia ('EFA'), a non-governmental organisation representing citizens' online liberties and rights, has consistently spoken out against the planned censorship, as has the similar Digital Liberty Coalition ('DLC') and the online political activism organisation GetUp! ('GetUp'). These three groups have collaborated and worked individually on a number of protest actions and organisation/mobilisation websites, including an Internet blackout campaign similar to that used by the CFF in the last week of January 2010 ('The Great Australian Internet Blackout') and online petitions. The three largest Australian ISPs have expressed disapproval of the planned legislature, on "technical, legal and ethical" grounds (Winterford & Hill 2008), with the managing director of one of them stating that Conroy "is the worst Communications Minister we've had in the 15 years since the [internet] industry has existed" (Malone, in Moses 2008). A number of opinion polls have also gauged wider public opinion on the filter as generally negative, especially amongst experienced Internet users and once respondents had been made aware of the limitations of the plans (Hearn 2010; LeMay 2010; Moses 2009a); although it must be noted that there have also been polls which measured general approval for the proposed filter ('Government websites hacked by Anonymous over censorship').

9.2 Anonymous, Operation Didgeridie and Operation Titstorm

Nevertheless, there is clearly ongoing and widespread opposition to the Australian Government's proposed censorship plans. However, Anonymous only entered this fray in late 2009 and early 2010, with two related instances of mobilisation into a hacktivist counterpublic. Due to their dispersed nature and presence on a number of Internet fora or channels, as well as the fact that they mobilised twice, they left many traces of their organisational and mobilisational activity online. However, given that our focus is on their external counterpublicity – that is, the elements of their mobilisation that effectively broke into a wider public of publics, the close analysis will centre on the central specially constructed text bearing their core 'intellectual ideology', with this ideology propelled into this wider public through their hacktivism.

9.2.1 Anonymous and Operation Didgeridie

Their first hacktivist mobilisation occurred on 09 September 2009 with 'Operation Didgeridie', a multi-pronged event utilising virtual sit-ins and fax and email floods. It was organised using the usual Anonymous channels (IRC and imageboards), but planning and co-ordination details and flyers were also distributed on insurgen.info, a wiki used to organise what Anonymous refer to as 'raids' (hacktivism and general nuisance making) ('Operation Didgeridie'), as well as another specially constructed website (09-09-2009.org, which is no longer online).

The Operation Didgeridie page provided a detailed rationale for the proposed hacktivism, outlining the scope and nature of the planned Internet filter, and referring to the major tenets of the more widespread opposition to the filter. The page explains that the filter will block "hundreds of legitimate sites" (including Encyclopedia Dramatica (ED), a satirical wiki much used by 4chan.org and

Anonymous, thus cutting off Australian members of Anonymous from the rest of the global collective). They also claimed that it would "slow down the Internet", which runs in direct opposition to Anonymous's constant assertions of the original hacker ethic that 'information is free'. Conroy (who Anonymous refer to irreverently as the "Minister of Interwebz Stuff") is described as "a stupid overbearing religious fanatic", and the government as "motherfucking censor-shits" who are worse than the Chinese government (perhaps the most widely criticised censorious regime), in that:

> NOT EVEN FUCKING CHINA HAVE BLACKLISTED ED!!!
>
> ('Operation Didgeridie')

The site also reproduces a large body of text from the 'No Clean Feed' website created by EFA, which provides detailed information on and suggestions for actions against the proposed filter. The material is bluntly identified as "shamelessly taken" from this site, and a hyperlink is provided, thus directing members of Anonymous to even more comprehensive information on the filter. The reproduced text highlights the broad range of concerns in play - that it will lead to 'overblocking', and that the blacklist is secret, and is thus open to the perpetration of current and future free speech abuses by the government. It points out that no other democracy has a comparable scheme, and asks whether Australians really want their nation to:

> …join a censorship club in which Burma, China and North Korea are the founding members?
>
> ('No Clean Feed: Learn', as cited in 'Operation Didgeridie')

It also gives evidence that the filter will significantly slow down Australian Internet access; that it will not be able to block most of the content it is primarily intended to combat (such as child pornography); that it will be easily circumvented; that it is a waste of taxpayer money; and that it is not supported by the majority of Australians. This intertextuality and evidence of wider opposition to the filtering scheme provided support for the cause as a legitimate one, and presumably worked to garner stronger participation in the Operation from the wider Anonymous counterpublic.

The importance of non-Australian members of Anonymous in the mobilisation is also stressed, through claims that if Australia enacts this legislation then the rest of the 'free world' may follow suit, thus affecting them all:

> YOU MIGHT SAY "YOU DONT CARE ABOUT AUSTRALIA" BUT IF THEY SUCCESSFULLY IMPLEMENT IT IN AUSTRALIA USA WILL FOLLOW SUIT UNTIL ALL THE FREE WORLDS HAVE NO FREE INFORMATION. This is of the highest importance we must save the internet… if [the filter] is 'successful', then it may spread.
>
> ('Operation Didgeridie')

The site also provided links to the specific virtual sit-in or DDoS software to be used, the URLs to be targeted (the Prime Minister's website, the ACMA website, and Conroy's Ministerial website) and the precise times for the attack (so as to ensure maximum critical mass). It also provided instructions and contact numbers and addresses for fax and email floods, requesting that these channels be inundated with anti-censorship messages, as well as asking members to call talk-back radio stations to air their anti-censorship views ('Operation Didgeridie'). Much like the CFF's website, the Operation Didgeridie site exhibits many of Stein's identified communicative functions (2009), although it is not intended for a wider public of publics with the aim of growing the Anonymous counterpublic (like the CFF site), but rather to co-ordinate and mobilise pre-existing members of Anonymous. It also once again illustrates the internal and external functions or orientations of counterpublics (Downey 2007), and the way in which counterpublics must

constantly work to negotiate and renegotiate their boundaries, thus generating a shared sense of investment and solidarity that can be translated into coordinated collective action.

9.2.1.1 Text

Operation Didgeridie was first publicly announced via YouTube on 08 August 2009 ('Message to the Australian Government'). This message was intended as a warning 'shot across the bows', as is detailed on the Operation's main page, which gave instructions to distribute the video link to media outlets to generate attention and thus hopefully provoke a response from the Australian government ('Operation Didgeridie'). If the government did not respond within the specified timeframe (which, unsurprisingly, they did not), then the instructions were to go ahead with the virtual sit-in and fax and email floods. It is unlikely that any response from the government (let alone the meeting of Anonymous's demands) was ever actually expected, and as such, the response window may be interpreted as primarily symbolic, providing an internal standard of behaviour for the counterpublic, and also giving them more time and a deadline within which to organise their hacktivist mobilisation and drum up publicity. Indeed, Anonymous themselves describe the lack of response as "long-known" and "long-expected", thus supporting this interpretation ('Operation Didgeridie'). The message text is reproduced below, with reference numbering.

> Hello, Kevin Rudd. We are Anonymous. We have been watching you. **(1)**
>
> It wasn't very long ago since you were elected, was it? The media hype surrounding your future government back in 2007 was incredible. Many of us Australians saw both you and Barack as beacons of potential to bring end to the conservative culture that currently swamps the USA and Australia. Many of us thought otherwise, and it turns out they were right. **(2)**

You, as a leader, have failed us. You are bringing an end to what is the greatest link between all people; the one thing that can cross all cultural boundaries, that can bring people together despite ethnicity, political or religious standings, class or nationality; the largest information transfer ever created. You, a democratically elected leader, have decided to do what only the most power-hungry of all tyrants dare:
You have opted to censor the internet. **(3)**

This is why we, Anonymous, have decided that this censorship plan should be among our primary targets for elimination. We have two demands that we consider central to our ideals: **(4)**

Firstly: We demand the abolition of the censorship plan proposed by the current government. This includes the removal of all targets on the blacklist, and complete abandonment of any further plans and endeavors by the Australian Government to censor the internet. **(5)**

Secondly: We demand the resignation of the Australian Minister for Broadband, Communications and the Digital Economy, Stephen Conroy. This is a man who has no level of understanding of the topic he is dealing with. This is a man who readily supports the abolition of free speech in exchange for social security. This man and his policies go against everything Australia and the western world stand for. As we see it, Stephen Conroy is completely unsuitable of being a minister of Australia, and as such, we demand his dismissal. **(6)**

Failure to meet these demands will result in our full-fledged wrath. This is not something you want to happen. **(7)**

Anonymous is your final obstacle in this battle. We fight where no one else dares to fight. We ruin the lives of animal abusers and bring pedophiles to justice. We destroy the reputation of political and religious leaders alike. Our soldiers currently fight the cult of Scientology and the Iranian government. To us, you are just a step higher. We will create and make freely available methods to render your censorship plan useless, and let these methods be known to the entire Australian public by ways we will not reveal in this message. We will also leak updated versions of the blacklist as often as we can, ensuring that the people who voted you in know what is being withheld from them. **(8)**

And as your people slowly begin to realize the veil that their own government is draping around them, they will realize that they voted a tyrant into power.
This is when we will have succeeded in all our goals. **(9)**

Information is free, Kevin. We, Anonymous, are not your friends. We are your doctors, your lawyers, your taxpayers, your brothers and sisters. We are everywhere. We may not be the best of people, but the one thing we will unceasingly fight for is the assertion that Information

is Free**. (10)**

Heed our demands, Kevin. This is our nation which you encroach upon.
These are uncharted waters for you and your colleagues. **(11)**

Farewell.
We are Anonymous.
We are Legion.
We do not forgive. We do not forget.
We are not your friends.
Expect us. **(12)**

The video overlays time-lapse footage of clouds, the Anonymous iconography of a headless (and thus anonymous) business-suited figure (see Figure 9), as well as static images of Rudd and Conroy. It is narrated by a computer-generated voice relaying a message directed at Rudd himself. The footage of clouds rushing overhead, the Anonymous businessman, and the robotic voice all contribute to their identification as an anonymous collective of faceless and nameless citizens – at no point do they show themselves as individuals. This anonymous self-presentation works to establish an image of them as both ubiquitous and ephemeral – they are nowhere and everywhere all at once. It also serves to underline the group's self-description as a kind of anti-individualistic hivemind – much like an ant colony, they would prefer we see them as a single entity rather than as networked individuals, with this image of mass singularity carrying more connotative weight and power than its networked counterpart. Their constant and heavy usage of the pronouns "we", "us" and "our", as well as their identification as an "it" or a single object repetitively underlines this collective solidarity.

Indeed, the only individuals shown are Rudd and Conroy, thus identifying them as the focus of the message and of Anonymous's collective intellectual ideology concerning the planned censorship. However, Prime Minister Rudd is unmistakably the primary intended recipient of the message. Anonymous hail him with "Hello", a very personal and conversational form of address (1), and refer to him by his Christian and surnames throughout, rather than by his formal title, 'The Honourable Kevin Rudd, MP' (1, 10, 11). This is arguably indicative of their lack of respect for him, in that they purposefully neglect to utilise his legal title, and instead address him as at least an equal, if not an inferior, if the rest of their missive is anything to

go by. However, it is also possible to interpret this over-familiarity and pseudo-friendliness as intended to connote a menacing proximity, particularly in combination with their self-presentation as ubiquitous and always observant. Whereas formal titles and forms of address establish hierarchies and distance, the combination of over-familiarity and menace serves to indicate that Rudd might be best to watch his back – indeed, as they later claim, their ranks could contain his neighbor, his doctor, or even his family.

Figure 10: A screen capture from the 'Message to the Australian Government' video

This direct, conversational tone is further highlighted through the use of a rhetorical question (2). They state that they have been watching him since his election, where he was widely perceived as a "beacon of potential", along with 'Barack' (who is also referred to colloquially rather than with honorary respect) (2). They describe both leaders as 'being seen' by many citizens as capable of bringing an end to the

"conservative culture that currently swamps the USA and Australia" (rather than definitively being capable of this) – referencing a (partial) public impression of them as emblematic of a progressive, positive politics that will bring their nations up and out of the repressive quagmire of conservatism (a current political situation that is asserted as fact). However, they then state that many of their members did not share this hope, implying that they were intelligent (or cynical) enough to pierce through a façade of political showmanship, before declaring that these suspicions did, indeed, 'turn out' to be well founded (2).

They then detail the reasons for this warranted distrust, directly inform Rudd of the fact that he is a failed leader of democratic people (including "us" - Anonymous) in that he is doing what "only the most power-hungry tyrants" do, and censoring the Internet. They thus counterpoise Internet censorship with democracy, and link it (and Rudd) with totalitarianism (3), effectively negating his status as a democratic leader. They describe the Internet factually as the ultimate unifying force, in that it is:

> the greatest link between all people; the one thing that can cross all cultural boundaries, that can bring people together despite ethnicity, political or religious standings, class or nationality; the largest information transfer ever created. (3)
>
> ('Message to the Australian Government')

They constantly identify Rudd ("you") as the active agent of this censorship, and indicate his actions are not forced but voluntary – he has "decided", "opted" and 'dared' to undertake a censorious regime (3), when he could have (and should have) decided otherwise. Anonymous portray Rudd and his government as purposively eradicating this unifying force and sharing of information (3), willfully generating segregation and information poverty, by "draping a veil" around (9) and "encroaching" on the Australian Internet (11). This use of metaphor and the verb "encroach" suggests that Rudd is darkening and isolating Australia's Internet

presence – the virtual Australia - and that he has no right to do so. It is not his to manipulate as he wishes; it belongs to and is of the people, not to 'leaders' masquerading as democratic representatives. This illegitimacy and lack of mandate is reinforced by the assertions that he is withholding information from those who voted for him (the wider public who collectively "own" him and his government, not the other way around) deceiving them into thinking they had voted a progressive leader into power when in actuality, they voted for a "tyrant" (9). His actions are thus doubly subversive – it is not only what he is doing, but also the way he is doing it that runs counter to democracy. Anonymously constantly reiterate throughout (via onscreen text) that "it does not like" what it is currently seeing, repetitively underlining their unified deep disapproval of Rudd's actions. Their use of the personal pronoun 'it' serves to further underline both their anonymous and unitary nature.

Anonymous state that this extremely negative state of affairs has thus become one of their "primary targets for elimination", thus informing us that they have several other ongoing engagements, and referencing their wider industriousness and interests. They declare that have two related demands that they see as central to their anti-censorship ideology (4). Their use of the imperative mood - demanding rather than asking - is an aggressive discursive move, implying that they feel their cause is strong enough and they possess enough power to be in a position to make such demands. This is, of course, not actually the case – their status and history as hacktivists, and therefore capable of disruption, but not actually holding any institutional authority or coercive power over the government, renders their demands infelicitous (Austin 1962). They are knowingly void performatives, carrying more of a symbolic than authoritative load. They are intended to express further components of Anonymous's intellectual ideology, and to generate an impression of authority or clout, without actually holding or generating the power necessary for their fulfillment.

Their first demand is that the planned filter is not just toned down or tweaked, but is utterly "abolished", or eradicated, and that all future plans for censorship are "completely abandoned" (5). There are to be no half measures here; they see Internet censorship of any kind as utterly and always objectionable. Second, they

demand that Conroy either resign or be dismissed from his ministerial position, signaling that they do not care how it happens, they just want him out of his office. They depict him as utterly ignorant, with "no level of understanding of the topic he is dealing with" and as being completely out of his depth – he does not understand the Internet or technical issues well enough to be attempting to enact its censorship (6). He will not only exchange free speech for "social security", but also do so "readily", or eagerly, privileging stability over democratic ideals (6). This statement brings to mind xxxs quote etc etc. He thus goes against all the ideals of Australia and the Western world, implying that he is more suited to authoritarian non-Western regimes such as China or Iran. When combined with these assertions, their repetitive use of the objectifying pronominal phrase "this is a man" in serves to amplify their distaste for him – he seems to be barely seen as human (6), and one can practically hear the contempt in their voices. All these declarations (like those pertaining to Rudd) use no modality whatsoever – they are asserted as simple fact or truth. The only non-factual statement is that Anonymous perceive or "see" Conroy as "completely unsuitable" for his Australian ministerial role, rather than asserting that he actually is unsuitable, but this perception is tied in to their previous factual declarations and their wider rationale for the necessity of his removal (6).

They go on to promise that failing to meet these demands will result in their 'full-fledged wrath" (7), which is warned of as something Rudd should wish to avoid as being akin to "uncharted waters", and thus unfamiliar and potentially dangerous (11). In doing so, they call to mind the world maps of antiquity that populated the then-unexplored oceanic regions with fabulous and terrifying creatures and the associated warnings that 'here be monsters'. The obvious deduction is that they are the beasts lurking within the unknown depths that the Prime Minister is already dipping his toes in, and that he would do well to retreat while he still has the chance.

They also describe themselves as a "final obstacle" in Rudd's battle, indicating that they realise he has already faced widespread opposition to his plans, but has traversed (or ignored) these previous obstacles (8). However, he is now faced with an unmovable and ubiquitous mass of anonymous citizens from all walks of life, including such reputable professionals as doctors and lawyers, therefore they should be taken seriously, as a sample of respectable society, rather than being dismissed as

a fringe group (10). They "are everywhere", are as close at hand as his brothers and sisters, and they pay the taxes that fund government activity, thus have the right to voice their opposition – indeed, they are Rudd's employers or superiors, despite his behaviour (10). This characterisation and connotations of enemy infiltration ties in with the menacing familiarity of their casual mode of address – Rudd had best watch his back as they may already have him surrounded. They go on to describe themselves as "Legion", an archaic mass noun with militaristic overtones raised to proper noun status through capitalisation, thus further emphasising the magnitude, strength and internal cohesiveness of their counterpublicity (12), and continuing the connotations of warfare. They neither forgive nor forget (12), but instead remain ever-vigilant – not only do they see themselves as a superconsciousness, they also as a kind of superconscience, monitoring society and keeping a track record of wrongs committed. They will never give up fighting for their core ideal of informational freedom (10), and they are most certainly not Rudd's friends (10, 12); rather, they constitute a formidable and persistent adversary.

They describe themselves factually and actively as "fighting where no one else dares to", "ruining" the lives of animals abusers and paedophiles (in reference to some of their past actions, where they posted the contact details of such individuals online), and "destroying" the reputations of political and religious leaders (with a clear reference to their anti-Scientology efforts). Indeed, they describe themselves as "soldiers" in the fight against Scientology and the Iranian government, both of whom are also perceived as engaging in Internet censorship (8). They clearly see themselves as involved in martial struggles against negative forces, with Rudd and his government being just one more, albeit slightly more powerful iteration of wickedness that they must overcome. The Australian government is thus implicitly equated to these other negative actors; indeed, they are not only as bad as paedophiles and authoritarian regimes, they are worse (presumably because they masquerade as a democratic entity).

Interestingly, their use of violently negative vocabulary to describe their involvement in this struggle has the effect of undermining the positivity of their self-presentation. This implicit recognition of their reputation for mischief and unpleasantness, even if they are fighting for a greater good, is underlined by their

self-admission that they "may not be the best of people" (10). They actively seek to establish themselves as a threat to the stability of the government and its censorship regime, drawing upon and even exaggerating their past actions and reputation, and promising that they will expose the Rudd government for the anti-democratic, deceptive and repressive force that it is (9), as well as creating and distributing software that will render any censorship actually undertaken impotent (8). They underline the imminence of these actions with their parting message to "expect us" (12). They take themselves rather seriously, as is evidenced through their formal and stylised self-presentation, as well as their use of archaic formal vocabulary such as "legion", "heed" and "farewell" (11, 12). They desire that Rudd do the same, warning that he should take their demands seriously, and let the hacker ethic of information freedom prevail (10) – or else. They see the Australian Internet as "their nation" (11) – a domain that belongs to citizens - thus further characterising governmental plans for censorship as illegitimate, and once more accentuating their claims to both represent and be constituted by 'the everyman' living next door, taking our blood pressure, or even sitting across from us at the breakfast table.

Anonymous thus use their video to comprehensively characterise Internet censorship and its agents in a deeply negative manner. The entire text is a concerted and strongly worded threat to the face of the government and its leaders – their actions are portrayed as deeply undemocratic and reprehensible, and worthy of no respect or obedience whatsoever. However, unlike the CFF and Hacktivismo, Anonymous are less concerned about how they themselves are perceived – they recognise that their reputation as not always politically-motivated trouble-makers may precede them, and seek to counteract any criticism along these lines by actively conceding their imperfections. They are content with establishing their motives in this instance as honourable, in that they are opposed to the destructive plans of the Australian government, and indeed, use the knowledge of their previous actions and aggressive self-description to imply that they are a dissenting force that should not be taken lightly. They have already proved that they are capable of causing disruption, and essentially promise to focus these disruptive capabilities on the Australian government unless Conroy and the proposed filter are abolished.

9.2.2 Anonymous's constellation of publics

9.2.2.1 The Australian Government

Once more, we can understand Anonymous as existing within a wider constellation of publics and counterpublics. The dominant public against which Anonymous direct their counterpublicity is clearly that of the Australian government, spearheaded by Prime Minister Kevin Rudd and Minister Stephen Conroy. While Anonymous are principally opposed to the Internet filter itself (as part of a broader opposition to Internet censorship of any kind), the government, and Rudd and Conroy in particular, are seen as the active agents of this proposed censorship, and are thus inherently bound up with the censorship itself. The Australian ISPs who have voluntarily adopted the filter, as well as all those technology firms involved with trials and the planned implementation of the filter, may be seen as collaborating with the government in this planned censorship. Although Google publicly opposed the filter on principle (despite their long-standing and only recently terminated kowtowing to the Chinese government's demands that they censor their search functionality within mainland China), the filter is no threat to established economic interests, and indeed, its installation would prove profitable to those corporations involved in its installation. Once again, the intersection of established political and economic interests and complicity creates a power bloc capable of overriding the principles of the freedom of speech and information in the online domain.

As in the case of the CFF, the government is perceived as a pseudopublic, displaying politics and its political intentions in front of Australian citizens but not facilitating or taking any notice of these citizens' attempts at ongoing participation in the political process. They are seen as undertaking a political project for which they have no mandate and which itself is inherently antidemocratic, and misleading the citizens they are ideally supposed to be democratically responsive to and thus

representative of. Indeed, despite the fact that they should be honestly serving the citizens who voted them in and pay their salaries, they are instead maintaining that the proposed filter is for 'their own good', when in fact, it is likely to have widespread and significantly negative immediate effects upon them, and open up future possibilities for further governmental abuses of free speech. Furthermore, they continue to display these political intentions in the face of widespread and significant opposition to the censorship, ignoring numerous national and international good arguments and advice regarding the many harmful likely outcomes of installing the filter, and persisting with their plans regardless – thus exposing the limits of the rational-critical Habermasian public sphere. Indeed, they are the epitome of a pseudopublic – they claim to speak for their members, but are in fact, entirely unresponsive and uninterested in any opinions but their own, despite the transmission of widespread dissent from the periphery of society towards their governmental core. Cracks in their hegemony have certainly emerged (Downey and Fenton 2002), but it would seem that the preceding instances of rational-critical deliberation and dissent have failed to truly exploit these fissures and exploit them to their fullest extent.

9.2.2.2 Networked counter/publics

As in the previous two cases, the Anonymous counterpublic is also oriented towards an interpublic engagement with a wider public of publics, primarily Australian, but also international when and where possible. They aspire to incite a wider discourse about the proposed Internet filter, and about the behaviour of the Australian government as a dominant public, and to have more citizens join the debate about internet censorship both in Australia and generally. They clearly see their role as educators, as is shown by their statements about exposing the government's anti-democratic betrayal of the "people" and the "Australian public" ('Message to the Australian government'). As in the previous cases, their counterpublicity is intended to be viral, provoking widespread preference reflection about the proposed

filter that will hopefully transform into preference alteration, and thus a generate a wider oppositional counterpublicity oriented towards the government. They do not necessarily want more citizens to join the Anonymous counterpublic – indeed, many citizens would not be interested in, capable of, or even approve of engaging in the day-to-day or occasional hacktivist activities of Anonymous. However, Anonymous hope to inspire the creation of new anti-filter counterpublics or for new members to join the existing counterpublics constituted by activist groups such as Get Up! and the EFA. The resonances between these groups and their discursive dissent generate discursive chains of equivalence, thus instantiating a discursively networked and collectively powerful public of counterpublics capable of fulfilling Downey and Fenton's expectations (2002), and exploiting or enlarging the existing fractures in the hegemony of the Australia government, hopefully bringing them to a state of total hegemonic destabilisation or crisis.

Indeed, they recognise that they are already part of such a modular network (Keane 2000) of counterpublics, as is evidenced through their reproduction of the anti-filter arguments from the EFA website ('No Clean Feed'). They utilise this borrowed discourse or intertextuality to both enrich their own internal solidarity and help inform their external counterpublic mobilisation, as well as establish a state of inter(counter)publicity via discursive resonance. Their hacktivism is therefore also intended to show solidarity with as well as gain wider externally-oriented publicity for this wider network of counterpublics, thus amplifying their collective discursive dissent. In fact, these feelings of solidarity are evidenced by a link posted on the Operation Didgeridie website after the Operation itself had occurred. The link is to a YouTube video summarising an anti-censorship campaign (as well as wider instances of criticism of the filter) built around an advertisement created by the GetUp!, which parodies the leading toothpaste brand name 'Sensodyne' ('Internet Censorship Australia'). The ad, which spread virally through Twitter (Moses 2009d), 'sells' a fictional toothpaste named 'Censordyne' which claims to offer "unproven, ineffective relief from Internet nasties" and a "fresh multimillion-dollar flavour", as well as prevent the dreaded "fast Internet". The videolink on the Anonymous website is accompanied by a rather jubilant message claiming that "Australia has received major attention from our project" (referring to the media

coverage of Operation Didgeridie) and expressing approval that 'they' (the rest of Australia) are "taking a stand on their own!" ('Operation Didgeridie').

9.2.3 Operation Didgeridie goes ahead

Although Anonymous's 'Message to the Australian Government' was given little attention during the month preceding the hacktivism itself, the eventual Operation, carried out on 9 September, served to propel its message into the wider public, through the media attention the hacktivism garnered. The video was not always referenced directly, but various other statements made by Anonymous, reiterating its core messages and tenets of their intellectual ideology (such as online flyers) were reproduced in the media coverage of their hacktivism. Although the Prime Ministerial (pm.gov.au) and ACMA (acma.gov.au) websites were, by all accounts, only overwhelmed by the virtual sit-in for a few hours at the most, and there was no mention of the fax and email floods, the operation received widespread media attention. Articles about the hacktivism were syndicated through many regional Australian newspapers and news websites, primarily through the national news agency, the Australian Associated Press ('PM's website hacked'). The event was covered by ninemsn.com ('Anonymous hacks PM's website'), News.com.au ('Kevin Rudd's website hacked over Internet censorship'), The Sydney Morning Herald (Moses 2009b) and The Age (Flower 2009) online, which regularly rank as the top Australian news websites according to Alexa ('Top Sites in Australia), and was also reproduced in New Zealand on the Stuff.co.nz website ('Aussie PM's website hacked by protester'). It also received television coverage on ABC News ('Rudd website attacked in filter protest'), 7 Network News ('Website hacked'), and Sky News ('PM's website hacked'), with the video being given considerable airtime in some cases, and was covered internationally by the popular online technology magazine Wired (Zetter 2009) and the online edition of the German magazine Der Spiegel, one of Europe's largest publications (Patalong 2009).

While the coverage often noted the illegality of the attacks and was critical of both the methods used to distribute Anonymous's intellectual ideology and some of the group's past actions, their anti-censorship message was often given support or acknowledged as a valid argument. Some (although generally those from less mainstream publications) even went so far as to suggest that Anonymous (whatever their methods and reputation) were, on balance, less reprehensible than the Rudd government; with the following quote being exemplary of such less common but nonetheless extant opinions:

> I legally can't say I'm in favor of what Anonymous is doing here, and I won't be participating in the raid, however there will be many who support any effort to highlight the Australian Government's attempt to introduce Chinese style censorship in a country that is suppose to be democratic and free.
>
> The means used here are illegal, but likewise so should any attempt to censor free speech in Australia be as well; Anonymous are no more criminals morally than the Rudd Government and Stephen Conroy are, and I wouldn't be the only person to suggest that Rudd and Conroy are the bigger criminals in this case.
>
> (Riley 2009a)

9.2.4 Anonymous and Operation Titstorm: A follow-up campaign

However, despite this coverage, Anonymous did not feel that Operation Didgeridie had been appropriately successful, in that the sites were brought down for so short a time. In an IRC discussion held during the sit-in, Anonymous members involved called it a failure in this sense, although they were happy with the media attention it received (Moses 2009b). As such, they indicated their plans for a second round of hacktivism shortly after Operation Didgeridie ended (Moses 2009c).

This second counterpublic mobilisation occurred 10 February 2010, and appears to have been organised using the usual Anonymous communicative fora such as imageboards and IRC channels, but it was also discussed in a thread on the primary Anonymous website ('Operation Titstorm: Why We Protest'). The planning was much more decentralised, with no evidence of a central website being used; instead, online flyers coordinating the event were disseminated using pre-existing channels of communication between Anonymous members (see Figure 10). The event built upon the expression of their intellectual ideology already generated by the YouTube video, but also responded to further developments to the governmental censorship regime.

Figure 11: The primary online flyer used to mobilise Operation Titstorm

This second instance of hacktivist counterpublicity, dubbed 'Operation Titstorm', appears to have been catalysed by accusations made by the Australian Sex Party (ASP). The ASP were formed in 2008 and run on a policy platform comprised in large part of opposition to the proposed filter, as well as policies of general tolerance of free sexual speech and expression, including gender and sexuality

equality, which they see as "hallmarks of free and democratic nations" ('Australian Sex Party Policies'). Conroy has banned access to the ASP website from within several governmental departments, including his own, with the ASP criticising these bans as unconstitutional and an "anti-democratic way of conducting debate", to no effect (Ozimek 2010).

In a press release dated 27 January 2010, the ASP revealed that under governmental direction, the ACMA was beginning to refuse to classify pornography depicting female ejaculation and involving small-breasted women. The application of the RC status is based on claims that the ejaculation is actually urination (which is banned under the classification guidelines), despite increasing scientific study of the phenomena and evidence to the contrary (as cited by the ASP), or on claims that it is 'abhorrent' (with male ejaculation eliciting no such reaction). The refusal to classify pornography involving small-breasted women stems from unclear classifications guidelines which state that pornography involving persons who "appear to be" underage must be refused classification, resulting in pornographic films involving women (established by mandatory FBI regulation to be well over 18) "being banned because they have an A cup size" (Patten 2010). The leader of the ASP argues that:

> Australian culture [is] being dumbed down in the sexual department and that political leaders [are] actively propagating an increasingly narrow window of acceptable sexual acts and cultures… all new appointees to the Classification Board and the Classification Review Board should undergo a short course in the latest scientific developments around sexuality and some sort of biology course to bring them up to date with the broad range of acceptable adult sexuality and body types.
>
> (Patten 2010)

There is some confusion over whether this statement and its resulting viral transmission around the Internet was particularly well-founded, or more the result of a kind of inverted moral panic stemming from the wider climate of opposition to the filter (Brown 2010), but it certainly caught the eye of Anonymous, whose members, as previously mentioned, interact on websites and fora often filled with

pornography of all kinds. The bans were seen as further evidence of the extension of the filter well beyond its stated aims of eliminating child pornography, and 'making a mockery' of filtering trials involving only a small ACMA blacklist, as the change in classification trends would potentially add millions of sites to the list, a concern when bandwidth has been established to slow in direct proportion to the number of sites blocked (Riley 2010a).

Rather than once more releasing a video warning indicating a month's period of grace to reconsider, Anonymous emailed a press release to Australian journalists and news websites the day before the planned mobilisation, apparently adjusting to the rapidity of the news cycle and presumably learning from their previous decision to give the Australian government a chance to respond. The release was addressed to "Australian Governmental officials, Members of Local and International Press, and the General Public", and was sent on behalf of Anonymous as a whole, with the usual collective pronoun "we" utilised throughout. It was reproduced in part (and occasionally in full; see Braue 2010) by various news reports prior to, during, and after the ensuing hacktivism, and drew strongly upon their central ideology, as already expressed in the previous 'Message to the Australian Government'. However, it also added in new criticisms related to the recent trend in pornography classification.

Anonymous again reiterated that they had been closely monitoring the activities of the Australian government over the last few years, "with particular focus on its stance towards Internet censorship". They declared that Australia's laws on Internet censorship were "already amongst the most restrictive in the western world", and that the government already filtered more content than "any other Parliamentary Democracy". They implied that Conroy's proposal to legislate mandatory national ISP filtering (with the goal being to prevent Australians from viewing "illegal and unwanted content") was evidence that he and "other elements within the Government" felt that they had not yet strayed far enough from democratic norms and the customary behaviours of other Western democracies.

Anonymous declared their concerns with the proposed legislature to be "two-fold". The first of their stated concerns was that Conroy's utilisation of the term "unwanted content" is "completely unacceptable" due to its ambiguity, with the

only possible interpretation of it simply being content that Conroy and the government do not want to be seen. This kind of ambiguously defined censorship based on complete governmental control is described as intolerable behaviour by any government, let alone a democratic one, with the release stating that "[n]o government should have the right to refuse its citizens access to information solely because they perceive it to be 'unwanted'".

Their second and 'more important' concern was with the "steps already taken by the Australian government to control what their populous [sic] sees", with specific reference to the recent furor over the refusal to classify pornography involving small-breasted women. Drawing on statements made by the ASP, they argue that classification officials are utilising ambiguous legislative wording to conflate legitimate and legal pornography with child pornography, and thus add this legal pornography to the filter blacklist. Echoing the ASP press release, they state that:

> Officials cannot claim that they believe the models in these movies are in fact underage, as the production the titles that have been affected are heavily regulated to ensure the age of the models.
>
> (Anonymous, in Braue 2010)

They go on to raise the point that "this censorship of a natural body type" may have negative repercussions upon the self-image of Australian women (a concern that one cannot help but take with a grain of salt), but are honest in stating that their main concern is that the Australian government is trying to "mess with [their] porn". This is, of course, an unacceptable restriction to the free and unhindered flow of information online, and they will ensure that the government "will learn" that this is the case. The press release ends with the usual Anonymous signature, that:

We are Legion.
We do not Forgive.
We do not Forget.
Expect us.

(Anonymous, in Braue 2010)

Given their past hacktivism against the Australian government and the dissemination of a flyer coordinating the event for the following day, this promise of further action was taken seriously by the government and the media, and served to build considerable publicity for the actual mobilisation. As promised, February 10 saw several governmental websites once again knocked offline by what appears to have been a mixture of virtual sit-in style tactics and server-side DDoS attacks, although the exact nature of the event is somewhat unclear. The information technology site The Register commented that the magnitude of the attacks was relatively low, and that they therefore appeared to be "hand-cranked rather than launched through zombie networks of compromised machines" (i.e. virtual sit-ins rather than server-side DDoS utilising botnets) (Leyden 2010a). However, other sources, including the Operation's discussion channel on the 'Why We Protest' site ('Operation Titstorm – Why We Protest'), cite extremely large numbers of page hits per second, and refer to the use of botnets in the attack (Johnston 2010, Zorz 2010).

Whatever the methods, the attacks were successful in overwhelming several governmental websites for a much longer period than during the previous Operation Didgeridie. The websites for the Australian Parliament House (APH) (www.aph.gov.au), the main Australian governmental website (www.australia.gov.au) and Communications Minister Stephen Conroy's Department of Broadband, Communications and the Digital Economy website (www.dbcde.gov.au) were knocked comprehensively offline for an extended period, and the APH site continued to drop intermittently offline throughout the day and was very slow to load when it was actually online (Riley 2010, 2010a). Kevin Rudd's website was reportedly defaced with pornography (Marks 2010), a wide range of government servers were "flooded with traffic", and various emails addresses within the Department of Parliamentary Services were also heavily

spammed with pornographic images and text (Davis 2010; Marks 2010; Moses 2010).

Although aware of the exact nature and timing of the disruptions, government officials were nonetheless powerless to prevent them, with their only strategy being to wait for the 'storm' to pass. A spokesperson for the Department of Parliamentary Services stated that "[o]ur objective has simply been to bring the site back into operation after the attack. They can't last forever" (in Zorz 2010). This was of course true; however, the APH website continued to be unavailable for most of the following two days (Davis 2010), with an Anonymous spokesperson going by the moniker 'Coldblood' stating that the action would continue until the group collectively decided it had gone on long enough:

> I believe that the government websites will remain down as long as we can keep them down. That could be anywhere from a few hours to a few months at the most… [the campaign will last] as long as the individuals that make up Anonymous decide that action needs to be taken to protect the freedom of the internet.
>
> (Anonymous spokesperson 'Coldblood', in 'Australia cyber-attacks could last 'months': hackers')

The attacks once again garnered widespread national and international media coverage. The Sydney Morning Herald gave extensive online exposure to the story ('Australia cyber attacks could last 'months': hackers'; Davis 2010; Moses 2010), and Asher Moses' series of articles were syndicated throughout several Australian news sites and were also carried by the New Zealand news site Stuff.co.nz (Moses 2010a). The Australian newspaper website ('Hackers 'titstorm' the PM and Parliament House'), ninemsn.com ('Anonymous brings down government websites'), ABC News ('Pro-porn protestors target government websites') and News.com.au ('Government websites hacked by Anonymous over censorship') also provided the Operation with national media attention, as did a wide range of blogs. Internationally, it was covered by several technology and computer security sites,

including The Inquisitr (Riley 2010; 2010a), The Register (Leyden 2010; 2010a), Ars Technica (Cheng 2010), ZDNet (Ho 2010), and Wired (Kravets 2010), and was also covered by the American Broadcasting Corporation ('Hackers disrupt Australian Government websites'), The Independent (Marks 2010) and multiple times by the BBC ('Australia websites hacked in porn filter protest'; 'Political hacktivists turn to web attacks'; Vallance 2010).

Although much of this coverage once again included criticisms of both Anonymous and their methods issued by both governmental officials and anti-governmental/anti-censorship bodies such as the EFA (e.g. Crozier 2010; Moses 2010), it did once again draw considerable public attention to the issue of Australian internet censorship and to the wider opposition to the government's plans. Media statements made by a spokesperson or several spokespeople for Anonymous articulated their belief in the effectiveness of the mediated counterpublicity generated by the attacks:

> "Maybe some people think the attacks are juvenile but it makes more of a message then signing a petition as the attacks cannot be ignored"… They said the aim of the attack was to make governments everywhere aware that they "can not mess with the internet and not have a backlash"
>
> (LeMay 2010a)

> The goal of today's attacks was to show the Australian Government that we are not afraid to act, and to raise awareness of the issue of internet censorship and our group's dedication to fighting it… Myself and the other protesters are quite satisfied with the results of our initial attacks.
>
> (Anonymous spokesperson, in 'Pro-porn protestors target government websites')

> [The campaign] allows us to impact something as large as a government with a handful of people… Going through the official channels you just get pushed aside, this way they have to listen…I believe it won't

> completely get the government to remove the filter they are planning on, but as long as something changes - for example the list (of banned sites) being made public - we will have succeeded anyway.
>
> (Anonymous spokesperson 'Coldblood', in 'Australia cyber-attacks could last 'months': hackers')

However, the spokesperson also stated that "the best thing the broader Australian public could do to protest against the filter was to sign the petition of Electronic Frontiers Australia and tell government officials that they disagreed with the policy" (LeMay 2010a), thus extending or underlining the counterpublicity of Anonymous's actions. This once more signals their recognition of their place within discursively networked public of counterpublics, and the increased counterhegemonic strength associated with such 'chains of equivalence' (Laclau & Mouffe 1985).

As in the case of Project Chanology, Anonymous intended to move towards offline protests in the week following Operation Titstorm, attempting to capitalise on the publicity garnered through their hacktivism and to gain wider participation in their counterpublicity. This activity was dubbed Project Freeweb, and was intended to provide a chance for Anonymous members all over the world to take their opposition to internet censorship to the streets. As Project Freeweb's organisation page made clear, Anonymous are extremely cognizant of the necessity for successful counterpublicity to interact with the mainstream media, with a spokesperson thating that Operation Titstorm was:

> …aimed at disrupting Australian government websites related to Conroy's little project in order to get the media and general publics' attention. This has been very effective tactic for Anon in the past and has once again paid off big-time for the mission, garnering hundreds of additional troops for Project Freeweb and generating an abundance of news stories in national and international media along with mostly unanimous support from citizen journalists in the blogosphere.
>
> ('Project Freeweb')

The Project Freeweb street protests were held all over Australia on 20 February 2010, but were not well attended (at least when compared with offline protests for Project Chanology). However, given that these protests were apparently a secondary addition to the media attention previously gained by Operations Didgeridie and Titstorm, it is perhaps hardly surprising that (as the organisation website put it in typical Anonymous tone), "[n]obody showed up and those that did fucked off to the pub within the first hour." ('Project Freeweb').

9.3 Access and control

Clearly, the discursive form of Anonymous's counterpublicity echoed the impoliteness inherent in the content of their discourse. Their disruptive and illegal political cracking-based Operations served to propel their intellectual ideology and its deliberate threat to the face of the Labor government into a much wider discursive arena than that provided by the usual channels of political dissent. It also served to amplify this ideology and its impoliteness by exposing the government as technologically inept, as well as giving them what might be best described as a taste of their own proposed medicine – effectively temporarily filtering their online presence out of existence. This rejection of the usual rational-critical rules and modes of political dissent vigorously challenged the apparent power and control of the governmental pseudopublic, thus subverting the usual patterns of access to important discursive channels and modes, and the power inherent within them. This counterpublicity was oriented towards provoking widespread political preference reflection and alteration, thus generating the registration of widespread anti-filter sentiment through more lawful communicative channels. It was also intended to show solidarity with the various other counterpublics involved in anti-filter protests, despite several of these counterpublics disapproving of Anonymous' methods.

9.3.1 Bypassing and manipulating the usual modes of communicative dissent to legislative changes

As discussed in the previous chapter, the usual modes of communicative dissent to legislative changes proposed by national governments (including voting, select committee submissions where available, and petitions) are fractured with problems. Their central failing is that they cumulatively advantage pre-existing power elites or dominant publics. Like the CFF's Internet Blackout, Anonymous's Operations generated their own highly public and non-externally mandated expressions of counterpublicity, simultaneously bypassing and manipulating these usual channels of dissent. They utilised various forms of hacktivism to generate this uncontrolled discursive counterpublicity, thus regaining control over all the levels of access to discourse, from planning through to the scope of their audience. By pre-alerting the news media to their planned Operations, they established a channel of access to a wide national and international audience for their intellectual ideology (albeit an audience somewhat contingent upon the overall success of their hacktivism). The launching of the ideology or discursive content of their hacktivism was contingent upon the success of its form, with success measurable by the magnitude of disruption and therefore media coverage.

Although Operation Didgeridie was only mildly successful in terms of disrupting the governmental websites it targeted, it was enough to ensure media coverage of the event, and thus effect the dissemination of Anonymous's message. The discursive content of their counterpublicity was launched into wider circulation by the DDoS attacks, with the form of the hacktivism itself underlining their ideology. Through knocking the governmental websites offline, even if only for an hour or so, Anonymous caused the government to appear technologically inept, in that they were unable to defend themselves from such attacks. The implication was that if they were incapable of defending themselves from such disruptions, how could they possible be entrusted with the administration and installation of a national Internet filtering system? Furthermore, if their governmental websites are so susceptible to such disruption, how reliable is such a system likely to be – surely it will be as

easily circumvented? Moreover, Anonymous's attacks effectively gave the government a taste of their own proposed medicine – effectively blacklisting the websites and their discursive content (if only temporarily), and censoring the dominant governmental publicity in favour of their own counterpublic discourse.

As such, the discursive form and discursive content of Operation Didgeridie worked in combination to 'hack into' the news media, thus mounting a powerful critique of the Labor government, threatening their face, and exploiting pre-existing fractures in their hegemony. This first Operation also served to prime the news media for the ensuing Operation Titstorm, in that the press release issued the day before the hacktivism began was taken seriously, and Anonymous's ideology was given coverage before the Operation had even commenced.

Due to its extended success in knocking several governmental websites offline, Operation Titstorm extended considerably upon the counterpublicity generated by Didgeridie. The fact that this second Operation overwhelmed governmental websites for a period of three days further underlined the technological ineptitude of the Labor government, once again garnering widespread media attention for Anonymous's discourse and intensifying the power of their counterhegemonic project. The previously discussed and widely reported admission from a Department of Parliamentary Services spokesperson that despite knowing that the attacks were imminent, they had no means of protecting themselves from them, further highlighted this technological vulnerability and lack of control. The other aspects of the hacktivism further underlined this technological critique, as well as adding a moral dimension relating to the reported over-censoring of pornography, with the inundation of the government with the very lewd material they were attempting to eradicate providing a further element of mockery to the situation.

Overall, the form of Anonymous's hacktivism both launched their intellectual ideology into widespread circulation, and underlined this ideology through its multi-faceted symbolic critique. Both Operations received widespread media coverage, both nationally and internationally, expanding hairline cracks in the governmental hegemony into full-blown fractures, and encouraging the expression of further dissent through more traditional channels. This latter goal was articulated by the spokesperson for Anonymous, who stated that "the best thing the broader Australian

public could do to protest against the filter was to sign the petition of Electronic Frontiers Australia and tell government officials that they disagreed with the policy" (LeMay 2010a), thus extending or underlining the counterpublicity of Anonymous's actions and contributing to the combined power of the modular network of anti-filter counterpublics, and signaling Anonymous's solidarity with this wider network.

9.3.2 The discursive construction of chains of equivalence

Despite these feelings of solidarity and the fact that Anonymous and other anti-filter counterpublics such as EFA and Get Up! share almost identical intellectual ideologies – that is, the content of their discourse exhibits strong resonance, to the extent that Anonymous reproduced statements and information disseminated by EFA, and expressed elation over the anti-filter campaign run by Get Up! – it is worth noting that these non-hacktivist counterpublics were disapproving of the form of Anonymous's counterpublicity. While supportive of their cause, they were extremely quick to distance themselves from the attacks through media statements, expressing concerns that Anonymous's methods would do more harm than good to the wider anti-filter campaign:

> Reports that attacks on Federal Government websites are being used to draw attention to the government's plan to introduce a mandatory Internet filter are alarming, and any illegal action of this nature must be condemned…By attempting to bring down or deface government websites, a minority of Internet users have brought negative attention to what is a very important issue for Australians.
>
> It would be much more helpful for these people to put their efforts behind legitimate action to stop this ineffective and inefficient attempt at censorship by the Australian government.
>
> (Stop Internet Censorship co-founder Nicolas Perkins, in Perkins 2010)
>
> EFA naturally condemns these attacks - not only are they illegal, but they damage the cause by playing to stereotypes of filter opponents as juveniles motivated by a desire to keep the Internet safe for porn. They serve no purpose but to give the Government the moral high ground,

> and distract from arguments about the ineffectiveness of the policy and its ramifications for free speech.
>
> It's easy to understand the frustrations that the Anonymous members feel - it's true that the censorship plan has been thrust on the Australian public without consultation, research or a coherent policy objective. But this campaign just serves for Anonymous members to get a little revenge. It certainly won't persuade anyone; rather, it will hurt the anti-filtering campaign.
>
> (EFA Chair Colin Jacobs, in Jacobs 2010)

There was also disagreement within the ranks of Anonymous itself, with a moderator in the Why We Protest online forum expressing concern over the use of DDoS attacks, and thus providing one instance amongst many of the incomplete internal reification of Anonymous's ranks:

> To those of you who are doing some sort of news piece on this or were directed here, read the WHOLE post before concluding this site's position on this
>
> (here's a hint, we don't like the censorship from Australia, but we don't condone the ddos attack from other portions of anonymous)…
>
> we don't support their ddos attack methods, as they will get people v&[40] and it doesn't get much support from the public (which is needed to stop the censorship)
>
> (Anonymous moderator RedOrbifold in 'Operation Titstorm – Why We Protest')

The Australian government themselves were (unsurprisingly) also extremely disapproving of the attacks, with a spokesperson for Minister Conroy describing them as "juvenile" (Flower 2010) and "totally irresponsible" in that they denied Australian citizens access to government resources located on the targeted websites

[40] v& is leetspeak for 'vanned', which refers to the unmarked vans used by the FBI and other law enforcement agencies to take away criminals. Therefore, 'people getting vanned' refers to people being arrested or taken away by the FBI or other law enforcement forces.

(Cheng 2010) – a rather hypocritical statement, one might argue! Furthermore, the disruptions were only temporary compared to the relative permanence of the planned filter, and as several commentators pointed out (including a spokesperson for Anonymous) analogous sit-ins and blockade actions occurring 'in real life' have long been seen as justifiable and valid forms of protest when traditional channels of dissent are perceived as inadequate:

> Communications Minister Stephen Conroy responded by branding those who carried out the attacks "irresponsible". This is the stock response of officialdom to direct action that causes any form of inconvenience: however, such action has a long and distinguished pedigree, with supporters arguing it is absolutely justified where existing political mechanisms do not give voice to a significant point of view.
>
> (Ozimek 2010)

> A DDoS attack occurs when a website is bombarded by requests for pages - often by a network of computers under the control of the hacker - effectively taking it offline. They are illegal in many jurisdictions.
>
> But a member of Anonymous told the BBC that in his view the attacks were a legitimate form of protest.
>
> "When truck drivers go on strike they block all the roads. It's the same principle," said the man who identified himself as "coldblood".
>
> (Vallance 2010)

Whether Anonymous's hacktivist counterpublicity had a net negative or positive effect on the campaign against and on general public opinion about the proposed filter is impossible to quantify, although there is no doubt that they did considerable damage to the government's hegemonic composure. However, the disagreement about their methods does raise the point that Laclau and Mouffe's theorised 'chains of equivalence' between counterhegemonic discursive projects or between counterpublics perhaps rely not only on resonance between the discursive content of these projects, but also the form of their discursive counterpublicity. Different groups see different forms of online protest counterpublicity as legitimate means to

achieving their stated cause, and the overall networked strength or solidarity of any public of counterpublics is likely to rely upon mutual approval of the forms of discourse utilised by those constituting the network as well as the ideologies or discursive content mobilised by these forms. This interplay between any given online political group's ideology and the specific technologies utilised in these ideology's organisation and mobilisation has received some preliminary attention (see Kavada 2009), but it is an issue that strongly compels further investigation.

9.4 The future of the Australian Internet

Shortly after Operation Titstorm, in early March 2010, The Labor Government announced that the Internet filter legislation was still in draft stage, and unlikely to be introduced into parliament for debate in time for the legislation to be passed (assuming it receives enough cross-Senate support, which is by no means assured) before the next Australian federal election (Berkovic 2010).

> The Government will take the time to ensure that it gets the legislative framework right… Discussion with ISPs and owners of high traffic sites on the implementation of ISP filters are ongoing. The Government is also considering the responses to the consultation paper on improved transparency and accountability measures which will feed into the legislative framework. The Bill will be introduced when these processes are completed.
>
> (Spokeswoman for Senator Conroy, in Riley (J.) 2010)

There was, unsurprisingly, some suspicion that the real reason for delay was due to "voter backlash" on the issue (Fitzgerald 2010), given the extensive counterpublicity directed at the Australian government by Anonymous and other activist organisations, coupled with critical receptions to other areas of their policy platform (primarily the mining tax).

At the time of writing, the deposition of Kevin Rudd as Prime Minister and leader of the Labor party by Julia Gillard has cast further doubt on the likelihood of the filter going ahead. Even if Labor win the 2010 election, they will lack the numbers to pass the filter legislation, with the Liberal-led coalition and Greens declaring their intent to vote against the policy or dump it in the case of election success ('Coalition to dump 'flawed' internet filter'). It appears that only time will tell whether the so-called 'Great Australian Firewall' will eventually be installed.

Chapter 10

Conclusion

10.1 Overview

10.1.1 Purpose, conceptualisation and inquiry

The core purpose or objective of this thesis has been to assess the phenomenon of hacktivism through a public sphere theoretical lens. However, the fulfillment of this goal necessarily generated two subsidiary objectives, in that both of the primary research concepts - 'hacktivism' and 'public sphere theory' – are rendered ambiguous by a multiplicity of divergent understandings and articulations. As such, both required considerable interrogation and definitive articulation and clarification before being combined and mobilised in the investigation and interpretation of empirical data, particularly the enduringly popular and continuously revised concept of the public sphere.

Prior to summarising the objects and methods of inquiry into this objective, it is fitting to say something of the original inspiration for and conceptualisation of the research project. At any level and scale, researching the role of media and communication in modern life presents an almost bewildering array of possible research objects, not to mention theoretical approaches. The sheer volume of media artifacts and systems increasingly permeating almost all aspects of daily life, particularly within developed and post-industrial nations but also within their developing and industrial counterparts, gives media researchers an incredible array of options from which to select subjects or objects of research that resonate with their personal interests and priorities. The predicament one faces is most definitely rooted in overabundance as opposed to scarcity.

So why hacktivism and the public sphere? To begin with, my interest in hacktivism was piqued by its (generally brief) mention in academic texts focusing on the increasing usage of the Internet for the organisation and mobilisation of a wide range of social and political activism. Further reading revelaed that there were relatively few texts dealing either exclusively or at least comprehensively with the phenomenon, and that these texts were being produced by a rather limited pool of authors who tended to repeatedly focus on the same incidences of hacktivism or hacktivist groups. Hacktivism, as an emerging form of activist communication, is understudied (hardly surprising, given its relative newness), and there is an ever-growing catalogue of hacktions that have completely escaped any examination whatsoever.

Furthermore, although there has been some consideration given to the interpretation of hacktivism as a democratically legitimate form of communicative resistance to the forces of elite power and control now "wander[ing] in absence on the electronic pathways" (CAE 1994: 23), primarily in the doctoral theses of Vegh (2003) and Samuel (2004), no focused or clearly articulated attention had been given to hacktivism through the lens of public sphere theory. In particular, there was a complete lack of interrogation into which strands of public sphere theory would best account for the phenomenon of hacktivism, thus allowing it to both be interpreted by and provide new directions for a theory of the public sphere more generally befitting of the modern mediated communicative environment. A detailed and clearly articulated public sphere theoretical approach to conceiving of hacktivism's contribution to political issues and discourses operating at multiple geopolitical levels, and of its constitution of an emergent form of communicative dissent to elite or hegemonic discourses was notably absent from the body of hacktivist/m research literature. As such, this uniquely unexplored nexus of communicative practice and theory provided the fresh research ground for this thesis.

Beyond the absence of attention given to this intersection, the inspiration for combining its two vectors stems from a long-standing fascination with and passion for the wider ecosystem of creative and avant-garde forms of resistance to the elite control of mediated discourse and deliberation, from various forms of alternative media publications and traditional offline forms of activism, to performance art,

graffiti and culture jamming. This interest is coterminous with a much broader enthusiasm for and belief in the importance of much more vigorous citizen participation in and discourse about political issues pertinent to us and the societies in which we live, both with one another and with our political representatives. To put it simply, I do not believe voting is enough.

This opinion can possibly be traced back to growing up amongst role models with a penchant for writing complaint letters to figures of authority, most notably politicians, and a wider familial belief in the importance of being outspoken about one's beliefs. The overwhelmingly *pro forma* responses to these letters and other polite and rational-critical forms of dissent have always struck me as both condescending and inadequate, hence my interest in more public and rowdy forms of opposition and political preference registration, which cannot be ignored or brushed aside to quite the same extent. Surely, truly egalitarian political communicative participation requires the opportunity not only to speak, but to speak in one's own preferred voice and to have one's political preferences widely heard and deliberated upon, both by other citizens and by those in positions of political or economic power.

This conviction underscores the attraction to public sphere theory, and while Habermas's work is completely deserving of the copious amounts of attention it has been paid, there is no escaping the fact that this attention rightly includes considerable quantities of critique and reformulation. Over the course of this project, the strength of my conviction in Fraser's call for an ongoing reconstructive project (2005) has intensified, as has my belief in the need for a synthesis of the postmodern, radical or agnostic theoretical tradition. This kind of synthesis is central to the articulation of a concept of the public sphere that accounts for the inherency of societal power stratifications and for an increasingly globally interconnected communicative environment.

Given their shared origins and points of similarity, it seemed natural to combine these fields of interest, and thus fill a research lacuna that appeared more than worthy of attention. Having broadly conceptualized the objects and theoretical mode of inquiry, the question then became one of which methodological framework to use. The vast majority of existing research into hacktivism utilised a

combination of descriptive case studies and interview data, with one instance of content analysis used to quantify the changing media perceptions of hacking and hacktivism pre- and post-9/11 (Vegh 2003). The methodology chapter of this thesis has already provided a detailed articulation of the process of deciding to utilise a qualitative method of inquiry, and in particular, to use a critical discourse analytical approach applied to three case studies, but it is useful and appropriate to re-summarise the main factors informing this decision here.

The use of case studies was informed both by their extensive usage in existing literature, and by the way in which a case study based approach allowed an in-depth investigation of a few purposively selected hacktivist incidents, rather than a glancing view of many. Samuel's hacktivist taxonomy (2004) provided an extremely useful scaffold for the theoretical sampling of the three cases used, but this sampling was also informed by a desire to address more recent examples of hacktivism, rather than relying purely on more well-known but increasingly dated hacktivist groups such as the EDT. Hacktivismo, the group focused on within the first case study, have received much previous attention within the existing literature, and as such, provided a robust and well-documented initial case with which to test the critical discourse analytical framework devised. However, the following two cases (the Creative Freedom Foundation and Anonymous) have, so far, received no or very little academic attention, thus fulfilling the goal of extending upon the existing body of hacktivist case study research.

Although the move away from using interview data and towards analysing the three hacktivist group's purposively constructed texts was certainly initially informed by difficulties with gaining interview access to hacktivists, this forced modification of the project's methodological approach has ultimately become a strength of this research. Although interview data has proved an important resource for other researchers of hacktivism, and should continue to be used as a resource wherever possible, relying on the textual artifacts produced by hacktivists to effect their counterpublicity rather than seeking out and generating new interview texts for analysis is actually more befitting of the intent of this thesis. What hacktivists say in private and their reflections upon their activity are somewhat irrelevant to an

investigation of the way in which they discursively construct counter*public* challenges to hegemonic or dominant publics or pseudopublics.

Furthermore, no previous attention has been given to hacktivism through an explicitly discourse analytical framework. Given that hacktivism is clearly an emergent form of multimodal discourse, which generates and utilises not only a large number of traditional linguistic texts, but also employs the many software and multimedia capabilities offered by the internet, it seems that that discourse analysis, critical or otherwise, provides an apt and peculiarly underutilized toolkit for its investigation and comprehension. Furthermore, critical discourse analysis provides the tools and theoretical underpinning needed to craft a flexible and sensitive methodological framework that allows the neo-Habermasian theoretical framework generated by the first research question to both interpret and be extended upon by the empirical case studies. Both the methodological and theoretical frameworks share a keen focus on issues of ideology and power, and on how discourse can be used to effect both the reification and challenge of these structures, thus they were easily amalgamated into a cohesive analytical lens capable of disclosing the information needed to answer the second research question.

10.1.2 Theoretical framework and research questions

The thesis had two primary research questions, the first of which generated the theoretical framework for the research. This question and the theoretical synthesis project providing its answer stem from Fraser's call (2005), much echoed by other public sphere scholars, for an ongoing reconstructive project that will not only remedy the practical and theoretical problems with the pre- and post-linguistic turn Habermasian conceptions of the public sphere, but will also continually bring the theoretical model into harmony with an ever-changing (particularly, an ever more global and mediated) communicative environment. This question identified the postmodern, radical, or agonistic public sphere theoretical tradition as being the most appropriate to this task, and was expressed as follows:

R1: How can the critical democratic intent behind the Habermasian ideal of the public sphere be reconciled with both:

a) the practical and theoretical criticism levelled at it, and

b) the diverse reconstructive projects undertaken within the 'post-modern' 'radical' or 'agonistic' public sphere and deliberative democratic theoretical traditions, which attempt to remain sensitive to issues of difference and power;

in a manner that generates a concise, holistic and operationalisable definition of the public sphere, that accounts and is appropriate for the modern mediated communicative environment?

This initial research question was answered through a process involving a thorough practical and theoretical critique of the traditional Habermasian conception of the public sphere, incorporating an articulation of the main tenets proposed within the postmodern, radical and agnostic reconstructive literature, and the subsequent delineation of the neo-Habermasian model – a concise and operationalisable definition of the public sphere that accounts for and is appropriate to the modern mediated communicative environment, and which provides a much heightened sensitivity to issues of power and difference.

The critique section began with an exploration of the historical inaccuracies or practical criticisms of the Habermasian public sphere as elucidated in *Structural Transformation*; specifically, Habermas's overidealisation of the internal function of the bourgeois public sphere; his lack of acknowledgement of the existence of multiple historical public spheres and of class- and gender-based exclusions inherent in the bourgeois public sphere; and his over-pessimistic analysis of the contemporary media and public sphere. Nancy Fraser's theoretical criticism of the Habermasian public sphere (1992) was then summarised, with her central principles subsequently providing a framework for an extended theoretical critique and reformulation based on the theorization of multiple public spheres (particularly the transnationalisation of the concept and the idea of counterpublic spheres); the

erosion of the theoretical barrier between public and private (including the impossibility of bracketing status differentials and the failure of rational-critical debate); the democratic advantages in allowing private interests into the public sphere; and the failures of the ideal of rational consensus.

It was made abundantly clear that there is a broad theoretical support base for a reworking of the public sphere concept in such a way as to enable it to much more adequately acknowledge societal power differentials, and to allow for the conceptualisation and interpretation of their contestation. The synthesis of these critiques and theoretical reformulations generated a definition for what is defined as 'neo-Habermasian public sphere theory', in that it retains the Habermasian public sphere as its departure point or core, but expands and sensitises it in order to effectively comprehend issues of power and difference. As Ryan requested, it allows publicness to "navigate through wider and wilder territory" (1992: 286).

Neo-Habermasian public sphere theory postulates the existence and recognition of multiple public spheres, operating at multiple levels and ranging in size from subnational to supranational (Keane 2000). These spheres are discursively defined against or in opposition with one another, and with the dominant or hegemonic public spheres within any given discursive or regional arena. As such, they should be referred to as counterpublic spheres, and are capable of operating as counterhegemonic projects. As Keane proposes, we should imagine a global modular network of interconnected and overlapping public spheres, linked not only by flows of resistance, but also by what Laclau and Mouffe term 'chains of discursive equivalence' (Laclau and Mouffe 1985; Mouffe 2000; 2000a; 2005).

Every public sphere, be it dominant or a counterpublic, is public in that it has an outwards orientation – it aims to engage with other publics – as well as an inwards, group solidarity-based orientation. Because the critique section reveals the demarcation of an *a priori* boundary around what issues may constitute public sphere discourses to be fundamentally exclusive, and exposes status bracketing or self-abstraction as a differentially distributed resource that re-privileges the already privileged, publics and especially counterpublics may be based around a range of concerns. Issues and concerns previously confined to the arena of the private may be brought into the public domain if they are discursively established as of

legitimate political importance, and may be fully articulated within their relevant public spheres. In effect, everything can be political if it is determined as such through discourse and deliberation.

Furthermore, the neo-Habermasian framework contends that exclusively privileging rational-critical deliberation as the only mode of legitimate communicative action within the public sphere is inherently and substantially exclusionary. As such, multiple modes of communication are deemed legitimate, including contestation and diverse forms of deliberation and debate. This communicative action does not necessarily need to be oriented towards the state, but can have powerful effects within civil society. However, these diverse modes of communication should still be judged in accordance with how well they fulfill a normative ideal of deliberative legitimacy. This 'deliberative authenticity' exists to the extent that communication induces reflection on preferences in a non-coercive fashion (Dryzek 2000, 2001). Finally, the achievement of truly rational consensus is seen as impossible in that it eliminates plurality, and any 'consensus' actually attained will always based upon exclusion and hegemonic stabilisation. 'Workable agreements' or temporary consensus will suffice, but should always remain open to contestation, with the processes of deliberation and contestation recognised as the truly valuable core of the concept of the public sphere.

This neo-Habermasian model provided the theoretical framework for the second research question, and for the empirical investigations into the nature of hacktivism's counterpublicity required to answer it:

> *R2: How does hacktivism, through discursively constructed and externally oriented publicity, function as a counterpublic sphere or counterhegemonic project oriented towards the provocation of political preference reflection and the destabilisation of a given dominant or hegemonic public?*
>
> *R2.1: How does the discursive **form** of hacktivism, as a counterpublic sphere or counterhegemonic discursive project, contribute to the*

provocation of political preference reflection and the destabilisation of a given dominant or hegemonic public?

*R2.2 How does the discursive **content** of hacktivism, as a counterpublic sphere or counterhegemonic discursive project, contribute to the provocation of political preference reflection and the destabilisation of a given dominant or hegemonic public?*

The neo-Habermasian theoretical framework was combined with a critical discourse analytical approach in order to analyse both the forms of and textual content produced by hacktivism, and thus answer these nested research questions. This attention to both discursive form and discursive content was structured by a focus on issues of diverse access to speech and attention and thus communicative power.

10.2 Findings and wider contributions

10.2.1 Findings: Research question 2

The findings or conclusions relating to the second research question draw from the empirical data generated by the case studies and critical discourse analysis conducted in Chapters 8 through 10. The question is best answered in a bottom-up fashion; that is, each subsidiary component is best discussed separately before summarising the findings relating to the broader question.

10.2.1.1 Research question 2.2: Discursive content

Research question 2.2 asks how the discursive *content* of hacktivism contributes to the counterpublicity or counterhegemonic projects generated by hacktivists, in order to provoke political preference reflection on a given issue and destabilise the dominant or hegemonic public dominating the wider discourse over or network of public spheres relating to the said issue. The close critical discourse analysis conducted upon the texts central to each of the three case studies provided the data relevant to this component of the research question, through its focus on ingroup-outgroup polarization, with the expected finding being that the hacktivists studied would routinely and fairly simply present themselves in a positive light in their textual artifacts, while simultaneously discursively constructing a negative portrayal of the groups they were opposed to.

However, the analysis revealed that this was not actually the case, and that the discourses of the hacktivists studied were, in fact, much more nuanced in terms of their construction and portrayal of ingroups and outgroups. Both Hacktivismo and the Creative Freedom Foundation invested considerable effort into constructing positive self-portrayals within their hacktivist discourse, but invested an equal amount of discursive work into making it clear that they were fighting for a cause, rather than against any specifically defined and negatively portrayed group. Certain actions, such as Internet censorship and the erosion of human rights online, were described in overwhelmingly negative terms, but there was little to no negative identification or naming of any particular groups (such as political parties or states).

This focus on a cause rather than on any exact opponent served various purposes. In the case of Hacktivismo, it ensures that their protest discourse remains up-to-date and appropriate to the evolving involvements of various nation states in the erosion and curtailment of digitally based human rights, and that it encompasses a broad and ever-changing roll-call of such offenders. In the case of the Creative Freedom Foundation, their focus on cause rather than any given New Zealand political party or Member of Parliament ensured that their protest was able to garner cross-spectrum support, and avoid alienating or offending the politicians they wished to

influence. It also reflected the inherited status of the Copyright Amendments Act (from the Labour party to the new National-led government).

However, no such delicacy or consideration of the face of their opponents was present in the anti-Australian Internet filter hacktivist discourse of Anonymous. As well as exhibiting a cause-orientation in the same manner as the two preceding cases, they painted Kevin Rudd, Stephen Conroy, and the Labor government as extremely negative in no uncertain terms. Anonymous invested considerable discursive effort into their explicit demonisation, with the offensive filter and its anticipated practitioners amalgamated into a holistic and much detested singular entity. Much work was invested in the construction of explicit and sustained threats to the face of Rudd and his colleagues, with Anonymous deliberately flouting the conventions of politeness and exhibiting marked disrespect towards their unambiguously identified adversaries. Interestingly, they also elected not to construct a positive self-presentation within their discourse, instead acknowledging their wider reputation as pranksters and deviants, and even mobilising this negative status in order to add weight and discursive power to their promises of hacktivist repercussions.

The differences in self- and other-presentation between the three groups may be attributed to a number of factors, some to do with the focuses of each instance of hacktivism and the practicalities inherent to these, and some to do with the reputation and nature of the hacktivists involved and the kind of hacktivist tactics they employed. As already discussed, Hacktivismo's software and protest is aimed at a number of nation state adversaries, hence it made practical sense for them to focus on cause rather than negatively portraying any particular one or number of these states within their discourse. Furthermore, although their software does allow its users to break some national laws, it is not illegal *per se*, and is intended to enforce the stipulations of Article 19 of the Universal Declaration of Human Rights. As such, their positive self-presentation is not undermined by criminality. The Creative Freedom Foundation's focus on cause rather than the negative portrayal of a particular opponent allowed them to garner cross-spectrum political support, avoid alienating the politicians they wished to influence, and took into account the inherited nature of the relevant legislation. As with Hacktivismo, their particular

hacktivist tactics were not illegal, ensuring that their positive self-presentation was also free of destabilizing criminal associations.

Conversely, Anonymous had a much more defined target in terms of the architects of the filter, which was reflected in the negative discursive construction of Rudd *et al*. The vehemence of this negative othering and their own ambivalent self-portrayal are also likely influenced not only by the fact that the group's wider status precedes them, but also because of the criminality of the hacktivist tactics they deployed in their two operations. DDoS attacks and page defacements are illegal actions, hence any positive self-presentation would have been undermined by this criminality, and any tempering of their discursive construction of the Labor government would have been rendered somewhat irrelevant.

Rather than being simple textual constructions based on the expected uncomplicated dynamics of ingroup-outgroup polarisation, the discursive content of the hacktivism of the three case groups was actually rather sophisticated and artfully constructed, taking into account a wide number of factors and drawing on many discursive strategies for effecting their intended portrayal of themselves, their causes, and their opponents. Although it is difficult to draw wider conclusions about the discursive content of hacktivism as a whole from three case studies, the lack of uniformity and the presence of reasonably equivalent levels of discursive sophistication and artistry does allow us to make the observation that hacktivists would appear to tend towards using the full discursive capabilities offered to them by the platform of the Internet, and by their relative freedom to construct rather elaborate, and in some cases, lengthy, protest discourses, in their efforts to provoke political preference reflection and destabilise the dominant or hegemonic publics or pseudopublics they oppose.

10.2.1.2 Research question 2.1: Discursive form

Research question 2.1 asks how the discursive *form* of hacktivism contributes to the counterpublicity or counterhegemonic projects generated by hacktivists, in order to provoke political preference reflection on a given issue and destabilise the dominant

or hegemonic public dominating the wider discourse over or network of public spheres relating to the said issue. Unlike the variety of strategies present in the content of the three case groups' discourse, the discursive form of their hacktivism served to provoke political preference reflection and effect the destabilisation of the relevant dominant or hegemonic pseudopublics in a broadly similar manner. Each of the three groups used the discursive form of their hacktivism to threaten the face of their adversaries by subverting (to greater and lesser extents, and through a variety of different tactics) the usual rules and norms of access to and control of widespread public political discourse on their chosen issues of contention.

These differing tactics and their effects have already been comprehensively detailed within Chapters 8 to 10; hence, a brief overview of the similarities and differences between each group's subversion of discursive access and control is sufficient for fleshing out this conclusion. All three groups used the form of their hacktivism to create the necessary spectacle for launching their discursive content into wider circulation – in effect, they used their communicative subversion to 'hack into' the mainstream media, and thus amplify their existing counterpublicity through garnering widespread reportage of their activities and discursively constructed intellectual ideologies. This accomplishment constitutes a final instance of subverting the usual norms of access to and control of discourse in and of itself, in that the mainstream media is overwhelmingly dominated by the discourses of dominant or hegemonic publics, and is thus more often a platform for the ideologies of political or economic elites rather than citizen minorities or counter-discourses. However, each case group generated their initial hacktivist spectacle of communicative subversion in a slightly different fashion.

Hacktivismo use their software to allow netizens, predominantly those in nation states with repressive and censorious digital regimes (such as China and Iran), to bypass their national firewalls and censors and thus both gain access to and contribute to repressed or prohibited information and discourses. In doing so, their software allows citizens to regain control over all levels of access to and control of the discourses they engage with online, thus undermining the otherwise total authority and control held by the leaders of their relevant nation states – it catalyses further counterpublicity in a self-replicating or viral fashion. This communicative

subversion constitutes a symbolic and practical threat to the face of these leaders and their dominant or hegemonic pseudopublic discourses, allowing dissenting citizens to bypass their authority, expose their lack of total control, and contribute to discourses criticizing such curtailment of the digital and human rights to free speech and expression. As detailed in Chapter 8, this face-threatening by way of the exposure of weakness and fallibility is also extended to the corporations involved in constructing and supplying the equipment needed for such firewalls and censorship, as well as to the allegedly non-repressive Western governments who stand idly by and implicitly sanction such corporate activity. This communicative subversion and attendant discursively constructed intellectual ideology, and their subsequent reportage in the mainstream media serves to provoke widespread political preference reflection and destabilise a variety of political-economic dominant or hegemonic pseudopublics through mounting a multivalent attack upon their public face.

The Creative Freedom Foundation used their viral Internet Blackout campaign to flood significant sections of New Zealand's Twitter and Facebook landscapes with blacked out avatars and links to their website, which details their intellectual ideology. This viral social networking was used to generate widespread subscription to the final phase of their campaign, in which participating websites and blogs redirected their homepages to a blacked out page within the Foundation's website which displayed a prepared statement explaining the reasons for the campaign and a link back to the site's homepage. The structure of the campaign generated a form of viral counterpublicity even more pronounced than that produced by Hacktivismo's software, in that it collected participants in a 'snowball' fashion, resulting in significant portions of the New Zealand Internet being blacked out in support of the Foundation's fight against S92. The participation of several notable opinion leaders and the overall levels of subscription to and visibility of the Internet Blackout not only generated an independent communicative channel for political dissent, and ensured widespread reportage of the Creative Freedom Foundation's intellectual ideology, but also flooded the typical channels of communicative dissent (such as petitions and emails to Members of Parliament) with much higher levels of subscription than usual, and put the weight of thousands of virtual bodies behind the Foundation's Select Committee submission. While the

content of their discourse remained carefully polite, this subversion of the norms of access to and control of public political discourse threatened the face of the National-led government and the corporate rights holders pushing for the adoption of the opposed legislation. Again, form and content combined to generate a multivalent, self-replicating and powerful counterpublicity that provoked widespread political preference reflection and alteration, thus destabilising the dominant or hegemonic pseudopublics and elite political-economic discourses driving S92.

Anonymous used a combination of repeated and various DDoS or flood attacks and website defacements to forcefully threaten the face of the Rudd government by undermining their credibility and authority, both by revealing their inability to maintain the integrity of their own web presence (let alone successfully and judiciously administer a national Internet filter), and by launching the face-threatening intellectual ideology contained within the discursive content of their hacktivism into a wide mass mediated circulation. As such, their Operations once more combined form and content to generate a multivalent and highly visible form of hacktivist counterpublicity that provoked widespread political preference reflection and worked to destabilise the dominant or hegemonic national governmental pseudopublic, and thus erode support for them and their planned filter.

In conclusion, it is apparent that hacktivist counterpublicity provokes political preference reflection and attempts to destabilise dominant or hegemonic publics or pseudopublics through a sophisticated and complex interplay between discursive content and form. The various discursive forms of hacktivism not only implicitly threaten the stability of dominant or hegemonic publics and pseudopublics through their subversion of the usual norms of access to and control of political discourse, but are also capable of generating the viral reproduction and spread of counterpublicity; of launching hacktivists' discursive content into wider circulation in the mainstream media; and of flooding existing channels of political dissent such as petitions and direct letters or emails to Members of Parliament with much higher subscription rates than usual. In other words, the various hacktivist tactics or discourse forms utilised serve as a platform for the hacktivists' intellectual

ideologies or discursive content, thus generating an emergent multivalent and multimodal discourse genre capable of generating a new mode of highly visible, often virally reproductive, and potentially very powerful protest counterpublicity.

10.2.3 Further similarities and differences

The previous sections have already made it clear that comparing and contrasting the three hacktivist groups provides a useful strategy for teasing out the conclusions to both of the subsidiary elements of the second research question. However, this excavation of similarities and differences is also productive in terns of drawing forth further conclusions and findings from the empirical research that do not fit neatly into a discussion of the discursive form and content of the three groups' hacktivism. Beyond these similarities and differences, there are also other underlying theoretical threads which have emerged as central to the project, and which warrant some attention and discussion.

10.2.3.1 Affinities between Hacktivismo, the CFF and Anonymous

Despite there being many differences between the three groups assessed, they also exhibited some striking philosophical similarities, particularly with regards to their opinion of the public value of their methods and their shared political-economic perspectives. Perhaps it is somewhat obvious, given that they voluntarily elected to use their given methods, but it is worth pointing our how clearly each group articulated their belief in the public value of their hacktivism, and in its ability to effect positive political change. Even Anonymous, despite acknowledging that they might not be 'the best of people' and that they have used their skills to less-than-progressive ends in the past, were adamant that their methods were ultimately in aid of the greater good, stating that they believed that any negative fallout from the

illegality of their hacktivism would be cancelled out by the negative publicity it also directed towards the Rudd government.

Each group also shared an almost identical orientation towards the global forces of neoliberalism and their influence on digital rights and freedoms in different national and regional locations all over the world. In particular, Hacktivismo and the Creative Freedom Foundation articulated almost identical anti-neoliberal ideologies, clearly identifying Western governments as completely in sway to the blind focus on profit and the maintenance of economic growth at all costs which forms the backbone of this political economic orientation. This ideological perspective was less apparent within the particular Anonymous Operations focused upon, but this underlying thread has emerged much more strongly in several of their more recent activities, such as their DDoS attacks against the RIAA website, as well as those against Visa and Mastercard. It would appear that hacktivism has very strongly inherited the anti-neoliberal opinions and beliefs that have been a core component of hacking since its first few generational iterations.

10.2.3.2 Philosophical differences

However, despite these similarities, the three hacktivist groups also exhibited some core differences in their underlying operational philosophies. Hacktivismo and the CFF quite obviously took great care to avoid engaging in any specifically illegal activities, as one would expect from their categorisation within Samuel's typology, and her identification that political coders (such as Hacktivismo) and performative hacktivists (such as the CFF) generally orient themselves in opposition to (elements of) mainstream society, but do not seek to exist completely outside these common socio-political structures or boundaries. They utilise their agency to test or push against these overarching structures, in the hope of modifying them into what they see as a more equitable or acceptable form, but they do not seek to drastically transgress, nullify, or ignore the existence of these structural boundaries.

Hacktivismo certainly seek to transgress against the boundaries and governing structures imposed by totalitarian regimes, but they are careful to maintain a respectful consideration of the ideals and agreed-upon core structures of Western democracies.

However, Anonymous show no such delicacy. As Samuel's typology indicates, they exhibit the lack of respect for cultural norms common to most political crackers, deliberately and almost gleefully flouting common laws and standards of behaviour and decency. While they are certainly cognizant the common structural boundaries of society they recognise them mainly through their deliberate transgression of these 'lines in the sand', using their anonymity to enable their operation in fields of illegal behaviour located far outside of what mainstream society deems acceptable. This basic lack of respect for the laws of the land places them at the most extreme end of the philosophical continuum inhabited by the three groups – a location that generates much disapproval but which is also quite possibly the best way in which to generate a maximum amount of publicity, given the intensity of the spectacle their hacktivism generates.

10.2.1.3 Differences in orientation to external definitions of hacking

These differences extend to the ways in which each of the groups orient themselves towards or against different external definitions of hacking, with Anonymous once more occupying the most extreme or *laissez faire* end of the continuum. Hacktivismo and the CFF seek to completely disown the dominant media discourse of the hacker as electronic criminal or bogeyman, with the CFF avoiding any explicit linkage with the terms 'hacker' or 'hacking' whatsoever. They mobilised much-domesticated tactical and visual elements of common hacking techniques in order to utilise the sense of the spectacular that they impart, but they avoided any kind of linguistic connection with the practice of hacking whatsoever, with the exception of a few news reports which noted the visual similarities between the Blackout and DDoS attacks. As such, they completely evaded entering into a

discussion about what exactly hacking is, and whose definition of the practice provides the most accurate reflection of reality.

In contrast, Hacktivismo clearly have no such sense of linguistic squeamishness, as their name indicates. Their software projects are also much more unmistakeably evidence of hacktivism's genetic connection with hacking. However, they also seek to disown, nullify, or subvert the dominant mass mediated discourse about hacking. They clearly articulate their subscription to the understanding of hacking as progressive proto-political exercise in aid of information freedom, with the hacker being a clever and somewhat rebellious but essentially altruistic figure engaged in enabling computers to be the mechanical agents of progressive social change. However, they do also exhibit a desire to borrow some of the publicity-friendly élan more commonly associated with the more criminal iterations of hacking, as is evidenced by their weak pseudonyms (e.g. Oxblood Ruffin, Grandmaster Ratte) and the rather grisly name of the parent group (Cult of the Dead Cow). These linguistic tactics lend their hacktivism a kind of subversive mystique that is somewhat missing from the self-presentation of the CFF, and which arguably makes many see them as somewhat more of a serious force to be reckoned with.

Anonymous clearly orient themselves much more firmly towards the 'electronic bogeyman' end of the definitional spectrum. They do not appear to care whether they are called hackers, cyberterrorists, cybercriminals or hacktivists, as long as they are taken notice of and given sufficient public attention and media coverage. Rather than trying to engage in reputation management at any significant level, they instead seem to rely on their causes speaking for themselves, and thus establishing their activities as being aimed towards a greater societal good and state of progressive technopolitics. They appear to actively court sensationalistic media descriptions that align them with the more criminal elements of hacking, welcoming the often intense publicity associated with the kinds of reportage this kind of 'naming' enables. One can only assume that they view the negative fallout as a necessary evil in garnering the kind of public exposure and thus counterpublicity they seek.

They also engaged in much discursive work aimed at countering the negative side-effects of courting this kind of attention, as did Hacktivism, with these self-

presentation efforts also intended to counter some of the problems linked with the use of anonymity or pseudonymity – specifically, the ways in which these nymity practices can engender suspicions of a lack of genuine political investment. The hacktivists sought to counteract these issues by aligning themselves with international human rights declarations and with "the people" or the masses; by stating that they come from all walks of life and therefore are a representative section of society; as well as doing much discursive work to undermine their opponents or what they are opposing. Again, this shows that hacktivists are extremely aware of how they and their actions may be perceived and take great care to try and secure communicative legitimacy for themselves.

10.2.4 Other findings and wider contributions

This thesis has also generated empirical, theoretical and methodological findings and advances relating to issues both extending from and beyond those focused on and explored by the second research question. These findings and contributions stem from the generative feedback loop constructed between the theoretical framework and empirical investigation, and are comprised of contributions made to both the broader field of hacktivism research, and also to the ongoing project of reformulating and extending upon public sphere theory.

10.2.4.1 Hacking into the mainstream

A more general finding emerging from the research is an intimation of the ways in which we might understand how hacktivist counterpublics (and indeed, counterpublics more generally) intervene in or cross over into dominant public spaces. Following on from Keane's elegant and intensely useful theorisation of a

global modular network of publics and counterpublics operating at multiple levels, and linked by both flows of resistance and also Laclau and Mouffe's 'chains of equivalence', our dominant mental image may be of counterpublics as existing in oppositional isolation from or to the dominant publics and discourses they seek to contest. However, considering the way in which the CFF and Anonymous mobilised their counterpublicity, this visual imaginary arguably requires some tweaking. Rather than visualising counterpublics as always retaining some kind of oppositional distance to the dominant or pseudopublic (see Figure 11.1 below, left section), we may in fact be better served by a visualisation along the lines of the diagram shown on the right of Figure 11.2:

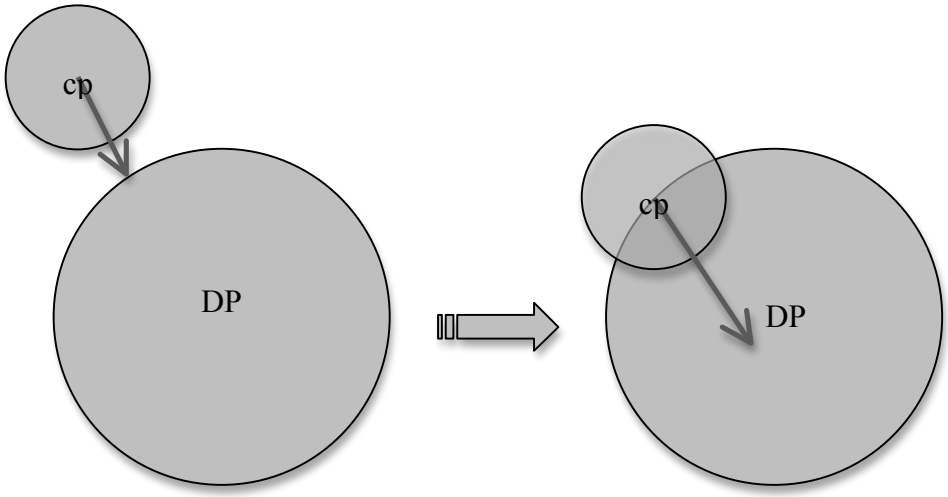

Figure 12: The relationship between hacktivist counterpublics (cp) and dominant publics (DP)

As Figure 11 attempts to depict, hacktivist counterpublicity, particularly that generated by the CFF and Anonymous, is perhaps best conceived of as fracturing the hegemony of dominant publics by inserting itself into the domains of these dominant spheres, and negotiating them on their own terms, rather than allowing these dominant publics to retain control of the rules of engagement. They do not challenge dominant publics just by butting up against them but remaining external, but by actually forcing their counterpublic into the midst of these dominant publics,

thus 'hacking into them' (and specifically, into the mainstream media) and thus fracturing them via internal rather than external pressure. Rather than adhering the Habermasian rational-criticality inherent in these dominant spheres, and thus enduring the failures of rational-criticality and the pitfalls of mass mediated refeudalisation, they force a renegotiation of the boundaries of political communication, thus embodying and providing support for the expansions and solutions neo-Habermasian theory provides.

10.2.4.2 Public sphere theory and human rights

Neo-Habermasian public sphere theory also provides an interesting evaluative perspective upon the rights-based discourse that has interwoven much of this thesis, from its instantiation in Levy's hacker ethics, to the focus on Internet rights and freedoms as a logical expansion of the existing framework provided by the united Nations and other entities. While the neo-Habermasian perspective shares many similarities with this rights-based discourse, it also highlights some shortcomings of this latter focus. The neo-Habermasian perspective goes much further than the rights-based perspective in that it speaks not only of the right to receive information and to articulate one's political opinions and engage in political deliberation, but it also focuses on and attempts to guarantee the right to be heard. Human rights-based discourses do not generally venture into this theoretical territory – the freedom to speak without persecution is seen as adequate, therefore it articulate a more negative conception of what free speech entails. That is, it sees free speech as reliant upon the right to speak without your speech being interfered with, whereas neo-Habermasian theory focuses on articulating a much more positive conception in which truly free speech only exists when we have secured not only the right to speak unimpeded, but also secured a guarantee that we will be heard. The rights-based discourse is thus rather devoid of considerations of power – it essentially boils down to the argument that "you have the right to say whatever you like but I have the right to completely ignore you", whereas the neo-Habermasian perspective is much more concerned with the act of listening as well as speaking.

10.2.4.3 Counterperformance?

This research has also identified the concepts of the spectacular and performative as entirely undervalued concepts within most public sphere theory, but as central to the agonistic and radical models that inform neo-Habermasian public sphere theory. At the most basic level, and in connection with the previous section of discussion, successful and effective deliberation rests upon the ability for its participants to get one another's attention. This is as it should be and as it has been for quite some time – theatricality has long been a central component of political deliberation and communication, as is evidenced by a long history of political theatre, art, cartoons, song, activism and films, and hacktivism simply represents a continuation of this historical thread of performativity. Arguably, the intention behind the utilisation of these concepts is that they not have any effect on deliberative authenticity whatsoever – they are intended as hooks, to reel in attention, with the political argument itself and claims of authenticity and reasoning either embedded within or drawn to the audience's attention by the performance.

No doubt there are those who will argue that politics should be serious and indeed, rational-critical, and for them, the element of performativity inherent in hacktivism is likely to make them unwilling to even listen to the argument being made by hacktivists. However, in doing so they are ignoring this long and varied history of performative politics, as well as the fact that our governmental or parliamentary politics is increasingly theatrical, largely due to its hypermediation. Indeed, there are so many different issues as well as frivolities clamouring for our attention and brain cycles within our modern society that the garnering of attention is growing ever-more difficult, thus theatricality, performance and spectacle is only likely to become more central to post-industrial politics.

As such, it is hardly surprising that hacktivism quite self-consciously exploits the aura of the outlaw and the theatricality that it inherits from hacking, using these facets, along with techniques borrowed from situationism and traditional activism as the hook to draw people's attention to their arguments and engage them in

deliberation. This not only allows hacktivists to speak, but also be heard – thus going some way towards combating the huge communicative advantages enjoyed by the political economic elites within our societies. As such, hacktivism arguably functions as a form of counter-performance. Indeed, in a refeudalised world where performative publicity dominates the global modular network of public spheres, this adoption of the dominant strategy (in combination with a genuine desire to catalyse political deliberation) would seem to be an extremely adroit move for any counterpublic, not just hacktivists. As such, a future direction for the refinement of neo-Habermasian public sphere theory will be to more firmly incorporate theoretical articulations of spectacle and performance, drawing upon the work of such theorists as Debord and the practice of situationism, thus hopefully enriching this theoretical lens even further.

10.2.4.4 Expanding empirical and theoretical resources

As previously discussed, hacktivism is a relatively recent phenomenon, and the state of research on the subject reflects this. Overall, there is a dearth of knowledge on and investigation and insight into hacktivist activity and groups, with what research there is stemming from a fairly limited pool of researchers. As such, one of the major contributions this thesis has made has been to add to the body of empirical knowledge of hacktivists, by conducting case studies into two previously ignored groups and their campaigns (the Creative Freedom Foundation and Anonymous). Furthermore, these case studies were located in Australasia, a location largely ignored within research into hacktivism. Finally, and perhaps most importantly, this thesis has established a new theoretical lens into the investigation of hacktivist activity. The neo-Habermasian perspective facilitates an understanding of hacktivism that not only addresses its contributions to the global modular network of public spheres, but is also able to effectively grapple with the issues of ideology, hegemony, and discursive power and difference that underline every hacktivist event.

However, this theoretical perspective was not only informed and influenced by its intended application to the empirical investigation of hacktivist case studies, but also extended upon by this case study research. The concept of viral counterpublicity was not originally conceived of by the neo-Habermasian theoretical framework, but was instead revealed or suggested by the case study research. However, the concept proved invaluable in the interpretation of the hacktivism investigated, and would be equally useful to the neo-Habermasian analysis of a wide range of counterpublic activity, primarily online but potentially offline as well. The empirical data and its analysis also revealed the potential inherent in the concept of 'chains of equivalence' between different but related counterpublics; hence, any future applications of neo-Habermasian public sphere theory to hacktivism and other forms of online counterpublicity should take care to remain attentive to these newly postulated components of the theoretical framework, as the viral spread of information and discourse and potential for interconnectivity are greatly facilitated by the networked structure of the Internet.

As such, perhaps the most significant achievement of this thesis has been its overall contribution to the ongoing project of reformulating and reimagining the theory of the public sphere. It has generated a concise and operationalisable model of the public sphere that is grounded within an extensive pre-existing body of theoretical critique and reconstruction, and which is both flexible and progressive enough to account for such emergent forms of communicative activity as hacktivism. Furthermore, its application to this phenomenon has added new concepts to the public sphere theoretical toolkit, thus expanding the model's functionality and sophistication with regards to comprehending the modern mass mediated communicative environment and the possibilities it enables for effective political dissent and counterpublicity. Certainly, the neo-Habermasian model should not remain static – the project of reformulation requires constant attention and theoretical dynamism and evolution – but it does provide a comprehensive framework that is both immediately useful and undoubtedly capable of continued refinement and extension.

10.2.4.5 Expanding methodological resources

Finally, this project has established some methodological innovations and advances that will hopefully prove useful to future researchers. The argument that software code should be accepted as a form of speech, and thus as a form of analysable discourse, is not one that has (to my knowledge) been made before, and potentially opens up a whole new domain of artifacts for discourse analysis and interpretation. Similarly, the identification of hacktivism as a fascinating and still-developing discourse genre will hopefully bring it to the wider attention of the many critical discourse analysts with an interest in political communication and the possibilities for so-called positive discourse analysis.

10.3 Limitations and recommendations for future research

10.3.1 Limitations

The primary limitations on this research were resource- (time, funding and manpower) and geography- or nationality-based. Hacktivism is an ever-expanding global phenomenon, and successful hacktivist events generate a diverse and often quite extensive corpus of possible texts for analysis. One researcher is simply incapable of keeping track of all the new instances of hacktivism around the globe, particularly given the linguistic divides in place. As such, the research was limited to focusing on English-speaking hacktivists operating in English-speaking nations, and was skewed towards my current location within Australasia. As previously mentioned, this is actually rather fortuitous, given the lack of research into

hacktivism within the region, but it should certainly be recognised as a limitation, if not a weakness, *per se*.

Obviously, the primary limitation stems from the time intensive and detailed nature of critical discourse analysis as a methodological strategy. This imposed limits on the number of cases that could be adequately interpreted or analysed using the given theoretical and methodological framework. Although I believe that the three cases used provide a strong template for the application of neo-Habermasian public sphere theory to hacktivism, there is no doubt that they are but a start. The investigation of more cases would have been preferable, but was prohibited by resource limitations, as well as word count constraints. Now that a theoretical and analytical framework has been established, more cases need to be addressed, and a wider understanding of hacktivism as neo-Habermasian counterpublicity established.

Finally, and to reiterate a limitation previously made clear in Chapter 2, the methodological approach utilised, while being extremely powerful in some respects, does have its own inherent limitations. Critical discourse analysis allows for a nuanced and sophisticated analysis that is able to comprehend the issues of power, ideology and difference so central to the neo-Habermasian theoretical framework, and which facilitates the smooth amalgamation of fine-grained empirical investigation and theoretical complexity and evolution. However, like all discourse analysis, it is inherently interpretive, which introduces aspects of subjectivity less apparent in more quantitative approaches. The incorporation of principles of systemic functional grammar or linguistics does go some way towards ameliorating this subjectivity, but can only go so far; hence, the analysis involved in this research is unavoidably infiltrated with my own conscious and unconscious interpretive biases. As such, I have attempted to make my ideological stance explicit throughout the research, as is standard for any critical discourse analyst hoping to excavate and expose the power relations inherent in discursive phenomena and texts, but am mindful that full transparency is an unattainable ideal.

10.3.2 Future research

Given these limitations, the ideal path for future research of this kind is fairly self-evident. More research power (time, funding and manpower) needs to be dedicated to investigating hacktivism as a contribution to the 'global modular network' (Keane 2000) of public and counterpublic spheres, and this research power needs to come from a variety of locations and incorporate much broader swathes of the world. Research collaborations between multiple researchers, based in geographically disparate locations and possessing a fluency in a wider range of languages would be the ideal. This is really the only way in which a cohesive investigation or series of investigations into hacktivism as global phenomenon can be achieved. Having more researchers dedicated to the task would also ensure that many more cases could be investigated, rather than continuing to languish in academic obscurity while Hacktivismo and their over-documented counterparts command the bulk of the attention! The critical discourse analytical approach would also be well-served by a multiplicity of co-operating researchers, as each member added to the team would provide an additional check-and-balance to the interpretive nature of this methodological framework, as well as contributing a more culturally diverse foundation for this interpretive work.

Having more research power would also increase the quantity of texts reasonably able to be subjected to the rather meticulous process of critical discourse analysis, thus enabling the analysis conducted upon each case study to become richer and deeper, as well as casting a wider net for the case studies selected. Although I believe critical discourse analysis provides a nuanced and sufficiently detailed and power/ideology-sensitive approach to investigating cases of hacktivism, it would also be useful (if one had access to sufficient research power) to combine it with a content analysis of the initial hacktivist texts, both private/organisational (if access to them was available) and publicly distributed, as well as to reportage of the hacktivist event. This would obviously require a research team capable of generating a sufficiently large but simultaneously cohesive sample of cases of hacktivism for it to be profitable to carry out such an analysis of the associated

texts, but if the resources and collaborative networks were available, it would allow for a rewarding inquiry into the protest topics most common to hacktivism, the vocabulary, memes and tones most commonly used in their discourse, the scope, content and tone of the responses to such events (following on from Vegh 2003), as well as allowing for cross-national comparisons between cases. Such data would help generate a much more comprehensive 'snapshot' of possible global commonalities between diverse hacktivist groups and practices, as well as exposing differences and possibly providing a way to begin quantifying what components or factors are necessary for hacktivists to optimise the counterpublicity or counterhegemonic discursive power they generate.

10.4 Finis

In closing, the process of conducting research for and crafting this thesis has been extremely rewarding, and its research objectives are worth continuing with and extending upon, both theoretically and empirically. There is no doubt that it has been a steep learning curve, and has, at times, seemed an almost impossible task, but I suspect this is the case for most, if not all, doctoral degrees. As my parents regularly suggest, perhaps one has to be a little mad to undertake one, and one of the major achievements would seem to be coming out the other end with one's sanity reasonably intact! However, such moments of doubt populate most worthwhile projects, and I find myself looking forward to using this research as a springboard from which to explore a whole host of new tangents and ideas. This, I think, is the strongest sign that the writing of a thesis has been a personally fulfilling achievement and an ultimately successful endeavour – that rather than being oversaturated with its subjects, one ends up being filled anew with enthusiasm for them, and itching to make a start on further research – to learn more, and to go further. After all, hacktivism certainly is not showing any signs of slowing down or stopping, and neither should research into the phenomenon. The same is undoubtedly true of public sphere theory; indeed, its functionality and value is

unwavering. As Fraser has stated, it is an "indispensable resource" for democratic theory (1992: 109), and as such, we have a responsibility to take the project of its reformulation seriously, and to see it as an ongoing journey rather than a destination.

Bibliography

A special message of hope: International bookburning in progress, 2001. Cult of the Dead Cow. Available at: http://www.cultdeadcow.com/cDc_files/declaration.html [Accessed May 8, 2010].

About Encyclopedia Dramatica. *Encyclopedia Dramatica*. Available at: http://encyclopediadramatica.com/Encyclopedia_Dramatica:About [Accessed May 25, 2010].

About Scoop. *Scoop*. Available at: http://www.scoop.co.nz/about/about.html [Accessed May 15, 2010].

About the Creative Freedom Foundation (CFF). *Creative Freedom Foundation*. Available at: http://creativefreedom.org.nz/about.html [Accessed May 13, 2010].

Abramson, J.B., Arterton, C. & Orren, G.R., 1988. *The electronic commonwealth: The impact of new media technologies on democratic politics*, New York: Basic Books, Inc.

Adams, R., 1996. The hacker: He may be a white hat, a black hat, a phreaker or a script kiddie. But is he just a vandal, or is he a modern-day hero? *New Statesman*, 129 (24-25).

'Addressing Security Council' (2002). United Nations: Addressing Security Council, Secretary-General Calls on Counter-Terrorism Committee to Develop Long-Term Strategy to Defeat Terror. Available at: http://www.un.org/News/Press/docs/2002/SC7276.doc.htm [Accessed June 1, 2001].

Agre, P.E., 2003. Growing a democratic culture: John Commons on the wiring of civil society. In H. Jenkins, D. Thorburn, & B. Seawell, eds. *Democracy and New Media*. Cambridge, MA: MIT Press.

Alexander, J.C. & Jacobs, R.N., 1998. Mass communication, ritual and society. In T. Liebes & J. Curren, eds. *Media, ritual & identity*. London & New York: Routledge, pp. 23-41.

Alger, D., 1998. *Megamedia: How giant corporations dominate mass media, distort competition and endanger democracy*, Lanham: Rowman & Littlefield.

Anderson, B., 1983. *Imagined communities: Reflections on the origin and spread of nationalism*, London and New York: Verso.

Anonymous brings down government websites, 2010. *ninemsn*. Available at: http://news.ninemsn.com.au/technology/1010636/anonymous-brings-down-

government-websites [Accessed August 18, 2010].

'Anonymous hacktivists say Wikileaks war to continue' (2010). *BBC.* Available at: http://www.bbc.co.uk/news/technology-11935539 [Accessed June 7, 2011].

Anonymous hacks PM's website, 2009. *ninemsn*. Available at: http://news.ninemsn.com.au/national/860067/prime-ministers-website-hacked [Accessed May 30, 2010].

Anonymous Iran. *Anonymous Iran*. Available at: http://iran.whyweprotest.net/ [Accessed May 25, 2010].

Apostolou, N., 2009. Kiwi's black out and blog off. *Digital Media*. Available at: http://www.digital-media.net.au/article/Kiwi-8217-s-black-out-and-blog-off/468516.aspx [Accessed May 15, 2010].

Aranowitz, S., 2000. Unions as Counter-Public Spheres. In M. Hill & W. Montag, eds. *Masses, classes and the public sphere*. London & New York: Verso, pp. 83-104.

Arquilla, J. & Ronfeldt, D., 2001. Afterword (September 2001): The sharpening fight for the future. In J. Arquilla & D. Ronfeldt, eds. *Networks and netwars: The future of terror, crime and militancy.* Santa Monica, Arlington & Pittsburgh: RAND, pp. 363-372.

Arquilla, J. & Ronfeldt, D., 2001a. Emergence and influence of the Zapatista netwar. In J. Arquilla & D. Ronfeldt, eds. *Networks and netwars: The future of terror, crime and militancy*. Santa Monica, Arlington & Pittsburgh: RAND, pp. 171-200.

Arquilla, J. & Ronfeldt, D., 2001b. The advent of netwar revisited. In J. Arquilla & D. Ronfeldt, eds. *Networks and netwars: The future of terror, crime and militancy.* Santa Monica, Arlington & Pittsburgh: RAND, pp. 1-28.

Arquilla, J. & Ronfeldt, D., 2001c. What next for networks and netwars? In J. Arquilla & D. Ronfeldt, eds. *Networks and netwars: The future of terror, crime and militancy.* Santa Monica, Arlington & Pittsburgh: RAND, pp. 311-362.

Arquilla, J. & Ronfeldt, D., 1993. Cyberwar is coming! *Comparative Strategy*, 12(2), 141-165.

Assange, J., 2006. The curious origins of political hacktivism. Available at: http://www.counterpunch.org/assange11252006.html [Accessed April 16, 2010].

Atton, C., 2003. Infoshops in the shadow of the state. In N. Couldry & J. Curran, eds. *Contesting media power: Alternative media in a networked world*. Lanham: Rowman & Littlefield Publishers, Inc., pp. 57-70.

Austin, J.L., 1962. How to do things with words. In A. Jaworski & N. Coupland, eds. *The discourse reader (1999)*. London & New York: Routledge, pp. 63-75.

Aussie PM's website hacked by protester, 2009. *Stuff.co.nz*. Available at: http://www.stuff.co.nz/world/australia/2851556/Aussie-PMs-website-hacked-by-protester [Accessed May 30, 2010].

Australia cyber attacks could last 'months': hackers. 2010. *The Sydney Morning Herald*. Available at: zotero://attachment/1395/ [Accessed August 18, 2010].

Australia websites hacked in porn filter protest, 2010. *BBC*. Available at: http://news.bbc.co.uk/2/hi/asia-pacific/8508732.stm [Accessed August 18, 2010].

Australian government internet censorship blacklist, 2009. *Wikileaks*. Available at: http://wikileaks.org/wiki/Australian_government_secret_ACMA_internet_censorship_blacklist,_18_Mar_2009 [Accessed May 26, 2010].

Australian Sex Party Policies. *The Australian Sex Party*. Available at: http://www.sexparty.org.au/index.php/policies [Accessed May 26, 2010].

Axford, B. & Huggins, R., 2001. *New media and politics*, London: Sage Publications.

Ayres, J., 1999. From the streets to the internet: The cyber-diffusion of contention. *The ANNALS of the American Academy of Political and Social Science*, 566(1), 132-143.

Baase, S., 2003. *A gift of fire: Social, legal and ethical issues for computers and the internet*, New Jersey: Pearson Education.

Bagdikian, B., 2004. *The new media monopoly*, Boston, MA: Beacon Press.

Bagdikian, B., 2000. *The media monopoly*, Boston, MA: Beacon Press.

Bakhtin, M., 1986. The problem of speech genres. In A. Jaworski & N. Coupland, eds. *The discourse reader (1999)*. London & New York: Routledge, pp. 121-132.

Barber, B.J., 2003. Which technology and which democracy? In H. Jenkins, D. Thorburn, & B. Seawell, eds. *Democracy and new media*. Cambridge, MA: MIT Press.

Barker, C. & Galasinski, D., 2001. *Cultural studies and discourse analysis*, London, Thousand Oaks & New Delhi: Sage.

Barlow, J.P., 1991. Coming into the country. *Communications of the ACM*, 34(3), 12-21.

Barney, D., 2003. Invasions of publicity: Digital networks and the privatisation of the public sphere. In L. C. O. Canada, ed. *New perspectives on the public/private divide*. Vancouver, Canada: University of British Columbia Press, pp. 8-22.

Barney, D., 2000. *Prometheus wired: The hope for democracy in the age of network technology*, Sydney, Australia: University of New South Wales Press.

Barrett, N., 1996. *The state of the cybernation: Cultural, political and economic implications of the Internet*, London: Kogan Page.

Baym, N., 2002. Interpersonal life online. In L. A. Lievrouw & S. Livingstone, eds. *Handbook of new media : Social shaping and consequences of ICTs*. London: Sage.

Blackout Homepage. *Creative Freedom Foundation*. Available at: http://creativefreedom.org.nz/blackout-homepage.html [Accessed May 21, 2010].

Becker, B. & Wehner, J., 2001. Electronic networks and civil society: Reflections on structural changes in the public sphere. In C. Ess & F. Sudweeks, eds. *Culture, technology, communication: Toward an intercultural global village*. Albany, NY: State University of New York Press, pp. 67-85.

Benhabib, S., 1996. Toward a deliberative model of democratic legitimacy. In S. Benhabib, ed. *Democracy and difference: Contesting the boundaries of the political*. Princeton, NJ: Princeton University Press, pp. 67-94.

Benhabib, S., 1996a. Introduction: The democratic moment and the problem of difference. In S. Benhabib, ed. *Democracy & difference: Contesting the boundaries of the political*. Princeton, NJ: Princeton University Press, pp. 3-18.

Bennett, T., 1986. Popular culture and 'the turn to Gramsci'. In O. Boyd-Barrett & C. Newbold, eds. *Approaches to media: A reader (1995)*. London, New York, Sydney & Auckland: Arnold, pp. 348-353.

Bennett, W.L., 2004. Communicating global activism: Strengths and vulnerabilities of networked politics. In W. van de Donk et al., eds. *Cyberprotest: New media, citizens and social movements*. London and New York: Routledge.

Bennett, W.L., 2003a. New Media Power: The Internet and Global Activism. In N. Couldry & J. Curran, eds. *Contesting Media Power: Alternative Media in a Networked World*. Lanham: Rowman & Littlefield, pp. 17-38.

Bennett, W.L., 2003b. Lifestyle politics and citizen-consumers: Identity, communication and political action in late modern society. In J. Corner & D. Pels, eds. *Media and the restyling of politics*. London, Thousand Oaks & New Delhi: Sage Publications, pp. 137-149.

Bentivegna, S., 2002. Politics and new media. In L. A. Lievrouw & S. Livingstone, eds. *The handbook of new media: Social shaping and consequences of ICTs*. Thousand Oaks, London and New Delhi: Sage Publications, pp. 50-61.

Berkovic, N., 2010. Rudd retreats on web filter legislation. *The Australian*. Available at: http://www.theaustralian.com.au/australian-it/rudd-retreats-on-passing-web-filter-legislation/story-e6frgakx-1225859630452 [Accessed May 25, 2010].

Billig, M. et al., 1988. *Ideological dilemmas*, London: Sage.

Böck, M., 2007. Reducing communicative inequalities: Toward a pedagogy for inclusion. In B. Cammaerts & N. Carpentier, eds. *Reclaiming the media: Communication rights and democratic media roles*. Bristol & Chicago: Intellect, pp. 66-86.

Boczkowski, P.J., 2004. *Digitalising the news: Innovation in online newspapers*, New York: Guildford.

Boczkowski, P., 2002. The development and use of online newspapers: What research tells us and what we might want to know. In L. A. Lievrouw & S. Livingstone, eds. *Handbook of new media: Social shaping and consequences of ICTs*. London: Sage, pp. 270-286.

Boggs, C., 2000. *The end of politics: Corporate power and the decline of the public sphere*, New York & London: The Guildford Press.

Bohman, J., 2007. *Democracy Across borders: From dêmos to dêmoi*, Cambridge, MA: The MIT Press.

Bohman, J., 2004. Expanding dialogue: The Internet, the public sphere and prospects for transnational democracy. In N. Crossley & J. M. Roberts, eds. *After Habermas: New perspectives on the public sphere*. Oxford: Blackwell Publishing.

Bohman, J., 1997. Deliberative democracy and effective social freedom: Capabilities, resources, and opportunities. In J. Bohman & W. Rehg, eds. *Deliberative democracy*. Cambridge, MA & London: The MIT Press, pp. 321-348.

Bohman, J., 1996. *Public deliberation: Pluralism, complexity, and democracy*, Cambridge, MA: MIT Press.

Boone, P., 1994. *Politics and the effectiveness of foreign aid*, London: London School of Economics.

Bourdieu, P., 1991. Language and symbolic power. In A. Jaworski & N. Coupland, eds. *The discourse reader (1999)*. London & New York: Routledge, pp. 502-513.

Bovine Dawn Dojo Forum. *Bovine Dawn Dojo Forum*. Available at: http://www.bovinedawn.com/index.php? [Accessed May 9, 2010].

Bowers, S., 1998. Information warfare: The computer revolution is Altering how future wars will be conducted. *Armed Forces Journal International*, August, 38-49.

Bowker, G.C. & Star, S.L., 1999. *Sorting things out: Classification and its consequences*, Cambridge, MA: MIT Press.

Bowman, S. & Willis, C., 2003. We media: How audiences are shaping the future of news and information. Available at: http://www.hypergene.net/wemedia/weblog.php [Accessed May 30, 2010].

Boyd-Barrett, O., 2004. Globalization, cyberspace and the public sphere. In P. Day & D. Schuler, eds. *Community practice in the network society: Local action/Global interaction*. London & New York: Routledge, pp. 23-35.

Boyd-Barrett, O., 2004a. U.S. global cyberspace. In D. Schuler & P. Day, eds. *Shaping the network society: The new role of civil society in cyberspace*. Cambridge: MIT Press.

Boyd-Barrett, O., 1995a. Conceptualising the 'Public Sphere'. In O. Boyd-Barrett & C. Newbold, eds. *Approaches to Media: A Reader*. London, New York, Sydney & Auckland: Arnold, pp. 230-234.

Boyd-Barrett, O., 1995b. Early theories in media research. In O. Boyd-Barrett & C. Newbold, eds. *Approaches to media: A reader*. London, New York, Sydney & Auckland: Arnold, pp. 68-76.

Boyd, C., 2008. Profile: Gary McKinnon. *BBC*. Available at: http://news.bbc.co.uk/2/hi/technology/4715612.stm [Accessed April 16, 2010].

Boyle, J., 1997. A politics of intellectual property: Environmentalism for the Net. *Duke Law Journal*, 47(87-116).

Brandenburg, H., 2006. Pathologies of the virtual public sphere. In S. Oates, D. Owen, & R. K. Gibson, eds. *The Internet and politics: Citizens, voters and activists*. New York: Routledge, pp. 205-222.

Brants, K. & Frissen, V., 2003. *Inclusion and exclusion in the information society*, European Media Technology and Everyday Life Network.

Brophy-Warren, J., 2008. Modest web site is behind a bevy of memes. *The Wall Street Journal*. Available at: http://online.wsj.com/article/SB121564928060441097.html [Accessed May 24, 2010].

Brown, P. & Levinson, S.C., 1999. Politeness: Some universals in language use. In A. Jaworski & N. Coupland, eds. *The discourse reader (1999)*. London & New York: Routledge, pp. 321-335.

Brown, R., 2009. High noon. *Public Address*. Available at: http://publicaddress.net/default,5693,the_public_bad.sm#post5693 [Accessed May 13, 2010].

Brown, R., 2010. The public bad. *Public Address*. Available at: http://publicaddress.net/default,5693,the_public_bad.sm#post5693 [Accessed May 14, 2010].

Brown, R., 2010. Has Australia really banned small breasts? *Crikey*. Available at: http://www.crikey.com.au/2010/01/29/has-australia-really-banned-small-breasts/ [Accessed May 30, 2010].

Bruns, A., 2007. Habermas and/against the Internet | Snurblog. Available at: http://snurb.info/node/621 [Accessed April 17, 2010].

Bryan, C., Tsagarousianou, R. & Tambini, D., 1998. Electronic democracy and the civic networking movement. In R. Tsagarousianou, D. Tambini, & C. Bryan, eds. *Cyberdemocracy: Technology, citizens and civic networking*. London & New York: Routledge, pp. 1-17.

BSA 1992 Schedule 5. *Australasian Legal Information Insititute*. Available at: http://www.austlii.edu.au/au/legis/cth/consol_act/bsa1992214/sch5.html [Accessed May 25, 2010].

Bunt, G.R., 2003. *Islam in the digital age: E-jihad, online fatwas and cyber Islamic environments* A. Karam & Z. Sardar, eds., London, Sterling & Virginia: Pluto Press.

Butsch, R., 2007. Introduction: How are the media public spheres? In R. Butsch, ed. *Media and public spheres*. Hampshire & New York: Palgrave MacMillan, pp. 1-14.

Calabrese, A., 2004. Toward a political economy of culture. In A. Calabrese & C. Sparks, eds. *Toward a political economy of culture: Capitalism and communication in the twenty-first century*. Lanham, Maryland: Rowman & Littlefiled Publishers, Inc., pp. 1-12.

Calabrese, A., 2000. Political space and the trade in television news. In C. Sparks & C. Tulloch, eds. *Tabloid tales: International studies on the tabloidisation of newspapers and television*. Lanham, MD: Rowman and Littlefield, pp. 43-62.

Calabrese, A., 1999. The welfare state, the information society, and the ambivalence of social movements. In A. Calabrese & J. Burgelman, eds. *Communication, citizenship, and social policy*. Lanham: Rowman & Littlefield, pp. 259-77.

Caldas-Coulthard, C.R., 1996. 'Women who pay for sex. And enjoy it.': Transgression versus morality in women's magazines. In C. Caldas-Coulthard & M. Coulthard, eds. *Texts and practices: Readings in critical discourse analysis*. London & New York: Routledge, pp. 250-270.

Caldas-Coulthard, C.R., 1994. On reporting: the representation of speech in factual and fictional narratives. In M. Coulthard, ed. *Advances in written text analysis*. London: Routledge, pp. 295-308.

Caldas, A. et al., 2008. Patterns of information search and access on the world wide web: Democratising expertise or creating new hierarchies? *Journal of Computer-Mediated Communication*, (13), 769-793.

Calhoun, C., 2004. Information technology and the international public sphere. In D. Schuler & P. Day, eds. *Shaping the network society: The new role of civil society in cyberspace*. Cambridge: MIT Press.

Calhoun, C., 1997. Nationalism and the public sphere. In J. Weintraub & K. Kumar, eds. *Public and private in thought and practice*. Chicago and London: The University of Chicago Press, pp. 75-102.

Calhoun, C., 1992. Introduction: Habermas and the public sphere. In C. Calhoun, ed. *Habermas and the public sphere*. Cambridge & London: The MIT Press, pp. 1-50.

Cameron, D. et al., 1989. Power/knowledge: The politics of social science. In A. Jaworski & N. Coupland, eds. *The discourse reader (1999)*. London & New York: Routledge.

Cammaerts, B., 2007a. Citizenship, the Public Sphere, and Media. In B. Cammaerts & N. Carpentier, eds. *Reclaiming the Media: Communication Rights and Democractic Media Roles*. Bristol & Chicago: Intellect, pp. 1-8.

Cammaerts, B., 2007b. Activism and media. In B. Cammaerts & N. Carpentier, eds. *Reclaiming the media: Communication rights and democratic media roles*. Bristol & Chicago: Intellect, pp. 217-224.

Cammaerts, B., 2007c. Media and Communication Strategies of Glocalised Activists: Beyond Media-Centric Thinking. In B. Cammaerts & N. Carpentier, eds. *Reclaiming the media: Communication rights and democratic media roles*. Bristol & Chicago: Intellect, pp. 265-288.

Cammaerts, B. & Carpentier, N., 2007. Introduction: Reclaiming the media: Communication rights and expanding democratic media roles. In B. Cammaerts & N. Carpentier, eds. *Reclaiming the media: Communication rights and democratic media roles*. Bristol & Chicago: Intellect, pp. xi-xviii.

Campos, G.P., Ramos, C.S. & Bernal, J.J.Y., 1999. Emotion discourse 'speaks' of involvement: Commentary on Edwards. *Culture and Psychology*, 5(3), 293-

304.

Carpentier, N., 2007a. Participation and Media. In B. Cammaerts & N. Carpentier, eds. *Reclaiming the media: Communication rights and democratic media roles*. Bristol & Chicago: Intellect, pp. 87-91.

Carpentier, N., 2007b. Journalism, media and democracy. In B. Cammaerts & N. Carpentier, eds. *Reclaiming the media: Communication rights and democratic media roles*. Bristol & Chicago: Intellect, pp. 151-156.

Carroll, W.K. & Hackett, R.A., 2006. Democratic media activism through the lens of social movement theory. *Media, Culture & Society*, 28(1), 83-104.

Castells, M. (2005). The Network Society: From Knowledge to Policy. In Castells, M. and Cardoso, G. (eds). *The Network Society: From Knowledge to Policy*. Washington DC, Center for Transatlantic Relations.

Castells, M., 2001. *The Internet galaxy*, Oxford: Oxford University Press.

CDC celebrates twelve years as a candle in the darkness, 1996. *Cult of the Dead Cow*. Available at: http://www.cultdeadcow.com/news/cdcanniv.txt [Accessed May 7, 2010].

CFF. *Creative Freedom Foundation*. Available at: http://creativefreedom.org.nz/ [Accessed May 13, 2010].

CFF announce Copywrong Song (CFF). *Creative Freedom Foundation*. Available at: http://creativefreedom.org.nz/story.html?id=117 [Accessed May 13, 2010].

CFF announce Internet Blackout against Guilt Upon Accusation laws, 2009. *Creative Freedom Foundation*. Available at: http://creativefreedom.org.nz/story.html?id=105 [Accessed May 14, 2010].

Center, P., 2004. Cable and Internet loom large in fragmented political news universe. *Pew Internet and American Life Project*. Available at: www.pewinternet.org/PPF/r/141/report_display.asp [Accessed May 30, 2010].

Chadwick, A., 2006. *Internet politics: States, citizens and new communication technologies*, New York and Oxford: Oxford University Press.

Chandler, A., 1996. The changing definition and image of hackers in popular discourse. In D. S. Wall, ed. *Cyberspace crime*. Aldershot & Burlington: Ashgate.

Chang, W., 2005. Online civic participation, and political empowerment: Online media and public opinion formation in Korea. *Media, Culture & Society*, 27(6), 925-935.

Charlesworth, A., 1993. Addiction and hacking. *New Law Journal*, April.

Cheng, J., 2010. Anonymous targets Australian government over porn filters. *Ars Technica*. Available at: http://arstechnica.com/tech-policy/news/2010/02/anonymous-targets-australian-government-over-porn-filters.ars [Accessed August 18, 2010].

Cheng, J., 2009. 4chan, eBaum's World carpet bombing YouTube with porn videos. *Ars Technica*. Available at: http://arstechnica.com/web/news/2009/05/4chan-ebaumsworld-carpet-bombing-youtube-with-porn-videos.ars [Accessed May 25, 2010].

Chester, J., 2007. *Digital destiny: New media and the future of democracy*, New York: The New Press.

Chester, J. & Larson, G.O., 2005. Sharing the wealth: An online commons for the non-profit sector. In R. McChesney, R. Newman, & B. Scott, eds. *The future of the media: Resistance and reform in the 21st century*. New York: Seven Stories Press.

Chilton, P. & Schäffner, C., 1997. Discourse and politics. In T. A. van Dijk, ed. *Discourse as social interaction (Discourse studies: A multidisciplinary introduction)*. London, Thousand Oaks & New Delhi: Sage, pp. 206-230.

Chomsky, N. & CBC Enterprises., 1989. *Necessary illusions: Thought control in democratic societies*, Montreal: CBC Enterprises.

Coalition to dump 'flawed' internet filter. 2010. *The Age*. Available at: http://www.theage.com.au/technology/technology-news/coalition-to-dump-flawed-internet-filter-20100805-11kmv.html [Accessed August 14, 2010].

Coleman, G., 2009. Code is speech: Legal tinkering, expertise and protest among free and open source software developers. *Cultural Anthropology*, 24(3), 420-454.

Coleman, G., 2004. The political agnosticism of free and open source software and the inadvertent politics of contrast. *Anthropological Quarterly*, 77(3), 507-519.

Colgan, P. & Elliott, G., 2010. Stephen Conroy and US at odds on net filter. *The Australian*. Available at: http://www.theaustralian.com.au/business/media/stephen-conroy-and-us-at-odds-on-net-filter/story-e6frg996-1225846614780 [Accessed May 26, 2010].

Connolly, T., Jessup, L.M. & Valacich, J.S., 1990. Effects of anonymity and evaluative tone on idea generation in computer-mediated groups. *Management-Science*, (36 (June)), 689-703.

Conroy, S., 2009. Measures to improve safety of the internet for families. *Minister*

for Broadband, Communications and the Digital Economy. Available at: http://www.minister.dbcde.gov.au/media/media_releases/2009/115 [Accessed May 25, 2010].

Coombe, R.J. & Herman, A., 2004. Rhetorical virtues: Property, speech, and the commons on the World Wide Web. *Anthropological Quarterly*, 77(3), 559-574.

Cooper, J. & Harrison, D.M., 2001. The social organisation of audio piracy on the Internet. *Media, Culture & Society*, 23, 71-89.

Copywrong Song: Remix Challenge and Open Call For Submissions. *Creative Freedom Foundation*. Available at: http://creativefreedom.org.nz/copywrong.html [Accessed May 15, 2010].

Costanza-Chock, S., 2005. The globalization of media policy. In R. McChesney, R. Newman, & B. Scott, eds. *The future of the media: Resistance and reform in the 21st century*. New York: Seven Stories Press.

Costanza-Chock, S., 2001. Mapping the repertoire of electronic contention.

Couldry, N., 2003. Beyond the hall of mirrors? Some theoretical reflections on the global contestation of media power. In N. Couldry & J. Curran, eds. *Contesting media power: Alternative media in a networked world*. Lanham & Oxford: Rowman & Littlefield Publishers, Inc., pp. 39-54.

Couldry, N. & Curran, J., 2003. The paradox of media power. In N. Couldry & J. Curran, eds. *Contesting media power: Alternative media in a networked world*. Lanham & Oxford: Rowman & Littlefield Publishers, Inc., pp. 3-16.

Couldry, N., Livingstone, S. & Markham, T., 2007. Connection or disconnection?: Tracking the mediated public sphere in everyday life. In R. Butsch, ed. *Media and public spheres*. Hampshire & New York: Palgrave MacMillan, pp. 28-42.

Coupland, D., 1995. *Microserfs*, London: HarperCollins.

Courtney, S., 2009. Pornographic videos flood YouTube. *BBC*. Available at: http://news.bbc.co.uk/2/hi/uk_news/8061979.stm [Accessed May 25, 2010].

Crawford, V.M., 1999. Discourse, identity and social action. *Culture and Psychology*, 5(3), 351-355.

Critical Art Ensemble, 2007. Digital Resistance: Explorations in Tactical Media. Available at: http://www.critical-art.net/books/ecd/index.html [Accessed May 30, 2010].

Critical Art Ensemble, 1996. Electronic Civil Disobedience and Other Unpopular Ideas. Available at: http://www.critical-art.net/books/ecd/index.html [Accessed May 30, 2010].

Critical Art Ensemble, 1994. The electronic disturbance. Available at: http://www.critical-art.net/books/ecd/index.html [Accessed May 30, 2010].

Crossley, N., 2004. On systematically distorted communication: Bourdieu and the socio-analysis of publics. In N. Crossley & M. Roberts, eds. *After Habermas: New perspectives on the public sphere*. Oxford & Massachusetts: Blackwell Publishing/The Sociological Review, pp. 88-112.

Crozier, R., 2010. Anonymous blasts Government sites for second day. *ITNews*. Available at: http://www.itnews.com.au/News/166993,anonymous-blasts-government-sites-for-second-day.aspx [Accessed August 16, 2010].

Crozier, R., Winterford, B. & Grubb, B., 2009. Conroy reveals plans to censor the internet. *ITNews*. Available at: http://www.itnews.com.au/News/162941,conroy-reveals-plans-to-censor-the-internet.aspx [Accessed May 26, 2010].

Cult of the Dead Cow. *Wikipedia*. Available at: http://en.wikipedia.org/wiki/Cult_of_the_Dead_Cow [Accessed May 7, 2010].

Cult of the Dead Cow: Main. *Cult of the Dead Cow*. Available at: http://w3.cultdeadcow.com/cms/ [Accessed May 7, 2010].

Cumming, S. & Ono, T., 1997. Discourse and grammar. In T. A. van Dijk, ed. *Discourse as social interaction (Discourse studies: A multidisciplinary introduction)*. London, Thousand Oaks & New Delhi: Sage, pp. 112-137.

Curran, J., 2005. Mediations of democracy. In J. Curran & M. Gurevitch, eds. *Mass media & society*. London & New York: Oxford University Press & Hodder Arnold, pp. 122-152.

Curran, J., 2004. The rise of the Westminster School. In A. Calabrese & C. Sparks, eds. *Toward a political economy of culture: Capitalism and communication in the twenty-first century*. Lanham, Maryland: Rowman & Littlefield Publishers, Inc., pp. 13-40.

Curran, J., 2003. Global journalism: A case study of the Internet. In N. Couldry & J. Curran, eds. *Contesting media power: Alternative media in a networked world*. Lanham: Rowman & Littlefield, pp. 227-242.

Curran, J., 2000. Rethinking media and democracy. In J. Curran & M. Gurevitch, eds. *Mass media and society*. London: Arnold, pp. 120-154.

Curran, J., 1998. Crisis of public communication: A reappraisal. In T. Liebes & J. Curren, eds. *Media, ritual & identity*. London & New York: Routledge, pp. 175-202.

Curran, J., 1991. Rethinking the media as a public sphere. In P. Dahlgren & C.

Sparks, eds. *Communication and citizenship: Journalism and the public sphere in the new media age*. London and New York: Routledge, pp. 27-57.

Dahlberg, L., 2007. The Internet and discursive exclusion: From deliberative to agonistic public sphere Theory. In L. Dahlberg & E. Siapera, eds. *Radical democracy and the Internet*. Hampshire & New York: Palgrave MacMillan, pp. 128-147.

Dahlberg, L., 2007a. The Internet, Deliberative Democracy, and Power: Radicalising the Public Sphere. *International Journal of Media and Cultural Politics*, 3(1), 47-64.

Dahlberg, L., 2007b. Rethinking the Fragmentation of the Cyberpublics: From Consensus to Contestation. *New Media Society*, 9, 827-847.

Dahlberg, L., 2005. The Habermasian public sphere: Taking difference seriously? *Theory and Society*, 34, 111-136.

Dahlberg, L., 2005a. The Corporate Colonization of Online Attention and the Marginalization of Critical Communication. *Journal of Communication Inquiry*, 29(2), 160-180.

Dahlberg, L., 2005b. Digital Democracy: Five 'Camps' Explored.

Dahlberg, L., 2004. Net-public sphere research: Beyond the first phase. *The Nation*, 11(1), 27-44.

Dahlberg, L., 2004a. Cyber-publics and the corporate control of online communication. *Javnost - The Public*, 11(3), 77-92.

Dahlberg, L., 2004b. Internet research tracings: Towards non-reductionist methodology. *Journal of Computer-Mediated Communication*, (9), 3.

Dahlberg, L., 2001. The Internet and democratic discourse: Exploring the prospects of online deliberative forums extending the public sphere. *Information, Communication, and Society*, (4(4)), 615-633.

Dahlberg, L. & Siapera, E., 2007. Introduction: Tracing Radical Democracy and the Internet. In L. Dahlberg & E. Siapera, eds. *Radical Democracy and the Internet*. Hampshire & New York: Palgrave MacMillan, pp. 1-16.

Dahlgren, P., 2007. Foreword. In B. Cammaerts & N. Carpentier, eds. *Reclaiming the Media: Communication Rights and Democratic Media Roles*. Bristol & Chicago: Intellect, pp. vii-x.

Dahlgren, P., 2007. Civic identity and net activism: The frame of radical democracy. In L. Dahlberg & E. Siapera, eds. *Radical democracy and the Internet*. Hampshire & New York: Palgrave MacMillan, pp. 55-72.

Dahlgren, P., 2003. Reconfiguring civic culture in the new media milieu. In J.

Corner & D. Pels, eds. *Media and the restyling of politics*. London, Thousand Oaks & New Delhi: Sage Publications.

Dahlgren, P., 2001. The public sphere and the Net: Structure, space and communication. In L. Bennett & R. Entman, eds. *Mediated Politics: Communication in the Future of Democracy*. Cambridge: Cambridge University Press, pp. 33-55.

Dahlgren, P., 2000. Media, citizenship and civic culture. In J. Curran & M. Gurevitch, eds. *Mass Media and Society*. London: Oxford University Press, pp. 310-28.

Dahlgren, P., 1995. *Television and the public sphere: Citizenship, democracy, and the media*, London: Sage.

Dahlgren, P., 1991. Introduction. In P. Dahlgren & C. Sparks, eds. *Communication and citizenship: Journalism and the public sphere in the new media age*. London and New York: Routledge, pp. 1-28.

Dahlgren, P. & Olsson, T., 2007. From public sphere to civic culture: Young citizen's Internet use. In R. Butsch, ed. *Media and public spheres*. Hampshire & New York: Palgrave MacMillan, pp. 198-209.

Dailey, D. et al., 2010. *Broadband adoption in low-income communities*, Social Science Research Council. Available at: http://www.ssrc.org/publications/view/1EB76F62-C720-DF11-9D32-001CC477EC70/ [Accessed May 6, 2010].

Dal, J., 2008. Neoliberal restructuring of the global communication system: Mergers and acquisitions. *Media, Culture and Society*, (30(3)), 357-373.

Daniel, J.O., 2000. Rituals of disqualification: Competing publics and public housing in contemporary Chicago. In M. Hill & W. Montag, eds. *Masses, classes and the public sphere*. London & New York: Verso, pp. 62-82.

Dartnell, M., 2003. Weapons of mass instruction: Web activism and the transformation of global security. *Millennium: Journal of International Studies*, 32(3), 477-499.

Davenport, T.H. & Beck, J.C., 2001. *The attention economy: Understanding the new currency of business*, Boston: Harvard Business School Press.

Davis, M., 2010. Porn fans attack website to protest against censorship. *The Sydney Morning Herald*. Available at: http://www.smh.com.au/technology/technology-news/porn-fans-attack-website-to-protest-against-censorship-20100212-nxmg.html [Accessed August 18, 2010].

Davis, R., 1999. *The Web of politics: The Internet's impact on the American political system*, New York: Oxford University Press.

Day, P. & Schuler, D., 2004. Prospects for a new public sphere. In D. Schuler & P. Day, eds. *Shaping the network society: The new role of civil society in cyberspace*. Cambridge: MIT Press.

Deane, J., 2005. Media, democracy and the public Sphere. In O. Hemer & T. Tufte, eds. *Media & glocal change: Rethinking communication for development*. Buenos Aires & Göteborg: Clascso & Nordicom, pp. 177-192.

DEF CON® hacking conference - The hacker community's foremost social network. *DEF CON*. Available at: http://www.defcon.org/ [Accessed April 16, 2010].

Deibert, R.J., 2003. Black code: Censorship, surveillance, and the militarisation of cybersapce. *Millennium: Journal of International Studies*, 32(3), 501-530.

Deibert, R.J., 2000. International plug'n'play? Citizen activism, the Internet, and global public policy. *International Studies Perspective*, 1(3), 255-272.

della Porta, D., 2005. Multiple belongings, tolerant identities and the construction of "another politics": Between the European Social Forum and the local social fora. In D. della Porta & S. Tarrow, eds. *Transnational protest and global activism*. Lanham: Rowman & Littlefield, pp. 175-203.

della Porta, D. & Diani, M., 2006. *Social movements: An introduction*, Malden, Oxford & Victoria: Blackwell Publishing.

Denning, D.E., 2001. Activism, hacktivism and cyberterrorism: The Internet as a tool for influencing foreign policy. In J. Arquilla & D. Ronfeldt, eds. *Networks and netwars: The future of terror, crime and militancy*. Santa Monica, Arlington & Pittsburgh: RAND, pp. 239-288.

Denning, D., 2000. Hacktivism: An emerging threat to diplomacy. *American Foreign Service Association*. Available at: http://www.afsa.org/fsj/sept00/Denning.cfm [Accessed May 26, 2010].

Denning, D.E. & Baugh Jr., W.E., 2000. Hiding crimes in cyberspace. In D. Thomas & B. D. Loader, eds. *Cybercrime: Law enforcement, security and surveillance in the information age*. London and New York: Routledge.

Devereux, E., 2007. *Understanding the media* 2nd ed., Los Angeles and London: Sage.

Devereux, E., 2003. *Understanding the media*, London: Sage Publications.

Diamond, L., 1992. Economic development and democracy reconsidered. In G. Marks & L. Diamond, eds. *Reexamining democracy: Essays in honour of Seymour Martin Lipset*. London: Sage Publications.

Diamond, L., Linz, J. & Lipset, S.M., 1988. *Democracy in developing countries*,

Boulder, Colorado: Lynne Rienner.

Diener, E., 1980. Deindividuation: The absence of self-awareness and self-regulation in group members. In P. B. Paulus, ed. *The psychology of group influence*. Hillsdale, New Jersey: Erlbaum.

van Dijk, J., 2000. Models of democracy and concepts of communication. In K. L. Hacker & J. van Dijk, eds. *Digital democracy: Issues of theory and practice*. London, Thousand Oaks & New Delhi: Sage Publications, pp. 30-53.

van Dijk, J. & Hacker, K., 2003. The digital divide as a complex and dynamic phenomenon. *The Information Society*, 19(4), 315-326.

van Dijk, T., 2009. Critical discourse studies: A sociocognitive approach. In R. Wodak & M. Meyer, eds. *Methods of critical discourse analysis*. London & Thousand Oaks, CA: Sage.

van Dijk, T., 2007. The study of discourse: An introduction. In *Discourse studies*. London: Sage, pp. xix-xlii.

van Dijk, T., 2006. Ideology and discourse analysis. In M. Freeden, ed. *The meaning of ideology: Cross-disciplinary perspectives*. London: Routledge, pp. 110-136.

van Dijk, T., 2002. Political discourse and political cognition. In P. A. Chilton & Christina Schäffner, eds. *Politics as text and talk: Analytical approaches to political discourse*. Amsterdam: Benjamins.

van Dijk, T., 2001. Critical discourse analysis. In D. Tannen, D. Schriffrin, & H. Hamilton, eds. *Discourse analysis*. Oxford: Blackwell, pp. 352-371.

van Dijk, T., 1998. *Ideology*, London: Sage.

van Dijk, T., 1997a. Discourse as interaction in society. In T. A. van Dijk, ed. *Discourse as social interaction (Discourse studies: A multidisciplinary introduction)*. London, Thousand Oaks & New Delhi: Sage, pp. 1-37.

van Dijk, T., 1997b. The study of discourse. In T. A. van Dijk, ed. *Discourse as Social Interaction (Discourse Studies: A Multidisciplinary Introduction)*. London, Thousand Oaks & New Delhi: Sage, pp. 1-34.

van Dijk, T., 1996. Discourse, power and access. In C. R. Caldas-Coulthard & M. Coulthard, eds. *Texts and practices: Readings in critical discourse analysis*. London: Routledge, pp. 84-104.

van Dijk, T., 1995. Aims of critical discourse analysis. *Japanese Discourse*, 1(1), 17-28.

van Dijk, T., 1995a. Discourse semantics and ideology. *Discourse and Society*, 6(2), 243-289.

van Dijk, T., 1995b. Discourse analysis as ideology analysis. In C. Schaffner & A. Wenden, eds. *Language and peace*. Aldershot: Dartmouth Publishing, pp. 17-33.

van Dijk, T., 1995c. Ideological discourse analysis. *New Courant*, 4, 135-161.

van Dijk, T., 1994. Discourse and inequality. *Lenguas Modernas*, 21, 19-37.

van Dijk, T., 1993. Principles of critical discourse analysis. *Discourse and Society*, 4(2), 249-283.

van Dijk, T., 1992. Discourse and the denial of racism. In Jaworski, A. & Coupland, N., eds. *The discourse reader (1999)*. London & New York: Routledge, pp. 541-558.

van Dijk, T., 1989. Structures of discourse and structures of power. In *Communication Yearbook*. Newbury Park, CA: Sage.

DLC. *Digital Liberty Coalition*. Available at: http://www.dlc.asn.au/ [Accessed May 26, 2010].

Doctorow, C., 2009. New Zealand netizens go black in protest of new "no-proof" copyright law that cuts off your Internet on accusation. *BoingBoing*. Available at: http://www.boingboing.net/2009/02/16/new-zealand-netizens.html [Accessed May 13, 2010].

Doctorow, C., 2009a. Cory Doctorow's #blackout tweet. Available at: http://twitter.com/doctorow/status/1226449926 [Accessed May 13, 2010].

Doctorow, C., 2008. Getting tough on copyright enforcers. *The Guardian*. Available at: http://www.guardian.co.uk/technology/2008/jul/01/internet.copyright [Accessed May 6, 2010].

Douglas, N., 2008. What The Hell Are 4chan, ED, Something Awful, And "b"? *Gawker*. Available at: http://gawker.com/346385/what-the-hell-are-4chan-ed-something-awful-and-b [Accessed May 24, 2010].

Downey, J., 2007. Participation and/or deliberation? The Internet as a tool for achieving radical democratic aims. In L. Dahlberg & E. Siapera, eds. *Radical democracy and the Internet*. Hampshire & New York: Palgrave MacMillan, pp. 108-127.

Downey, J. & Fenton, N., 2003. New media, counter publicity and the public sphere. *New Media & Society*, 5(2), 185-202.

Downey, J. & Fenton, N., 2002. Counter public spheres and global modernity.

Downing, J., 2003. The Independent Media Centre movement and the anarchist socialist tradition. In N. Couldry & J. Curran, eds. *Contesting media power: Alternative media in a networked world*. Lanham: Rowman & Littlefield,

pp. 243-258.

Downing, J., 2001. *Radical media: Rebellious communication and social movements*, Thousand Oaks, London and New Delhi: Sage Publications.

Doyle, G., 2002. *Understanding media economics*, London: Sage.

Doyle, G., 2002a. *Media ownership: The economics and politics of convergence and concentration in the UK and European media*, London: Sage.

DRM Free New Zealand. *Creative Freedom Foundation*. Available at: http://creativefreedom.org.nz/drm-free.html [Accessed May 16, 2010].

Dryzek, J.S., 2006. *Deliberative global politics*, Cambridge & Malden, MA: Polity Press.

Dryzek, J., 2001. Legitimacy and economy in deliberative democracy. *Political Theory*, 29, 651-668.

Dryzek, J., 2000. *Deliberative democracy and beyond: Liberals, critics, contestations*, Oxford: Oxford University Press.

Duff, L. & Gardiner, S., 1996. Computer crime in the global village: Strategies for control and regulation - In defence of the hacker. In D. S. Wall, ed. *Cyberspace crime*. Aldershot and Burlington: Ashgate.

Dutton, W. & Helsper, E., 2007. The Internet in Britain 2007. Available at: http://www.oii.ox.ac.uk/research/oxis/OxIS2007_Report.pdf [Accessed May 30, 2010].

Dyer-Witheford, N., 2007. Hegemony or multitude? Two versions of radical democracy for the Net. In L. Dahlberg & E. Siapera, eds. *Radical democracy and the Internet*. Hampshire & New York: Palgrave MacMillan, pp. 191-206.

Dyer-Witheford, N., 1999. *Cyber-Marx: Cycles and circuits of struggle in high technology capitalism*, Illinois: University of Illinois Press.

Edwards, D., 1999. Emotion discourse. *Culture and Psychology*, 5(3), 271-291.

Edwards, G., 2004. Habermas and social movements: What's new? In N. Crossley & J. M. Roberts, eds. *After Habermas: New perspectives on the public sphere*. Oxford: Blackwell Publishing.

van Eemeren, F.H. et al., 1997. Argumentation. In T. A. van Dijk, ed. *Discourse as social interaction (Discourse studies: A multidisciplinary introduction)*. 1997: Sage, pp. 208-229.

EFA. *Electronic Frontiers Australia*. Available at: http://www.efa.org.au/about/ [Accessed May 26, 2010].

EFF: Electronic Frontier Foundation. *Electronic Frontier Foundation*. Available at: http://www.eff.org/ [Accessed May 2, 2010].

EFF's Staff. *Electronic Frontier Foundation*. Available at: http://www.eff.org/about/staff [Accessed May 8, 2010].

Einhorn, B., 2002. Hackers to Beijing: Have a cow! *Business Week*. Available at: http://www.businessweek.com/technology/content/aug2002/tc2002085_2375.htm [Accessed May 7, 2010].

Eley, G., 1992. Nations, publics, and political cultures: Placing Habermas in the nineteenth century. In C. Calhoun, ed. *Habermas and the public sphere*. Cambridge, MA & London, England: The MIT Press, pp. 289-339.

Elliott, P., 1982. Intellectuals, the 'information society' and the disappearance of the public sphere. In O. Boyd-Barrett & C. Newbold, eds. *Approaches to media: A reader (1995)*. London, New York, Sydney & Auckland: Arnold, pp. 260-262.

Elshtain, J.B., 1997. The displacement of politics. In J. Weintraub & K. Kumar, eds. *Public and private in thought and practice*. Chicago and London: The University of Chicago Press, pp. 166-181.

Eschenfelder, K.R. et al., 2005. Global copyright protest? A comparison of DeCSS posting in the People's Republic of China, Hong Kong, and the European Union. In *38th Hawaii International Conference on System Sciences*. Hawaii. Available at: http://www.cdsl.computer.org/comp/proceedings/r>hicss/2005/2268/05/22686133b.pdf [Accessed May 30, 2010].

Etzioni, A., 2003. Are virtual and democratic communities feasible? In H. Jenkins, D. Thorburn, & B. Seawell, eds. *Democracy and new media*. Cambridge: MIT Press.

Evans, C., 2002. Copyright and the Net. In D. Cummings, ed. *The internet: Brave new world?* London: Hodder & Stoughton.

Evers, S., 1996. Information warfare: Stopping the hacking of cyber information. *Jane's Defense Weekly*, 25(15), 22-25.

Fairclough, N., 2009. A dialectical-relational approach to critical discourse analysis. In R. Wodak & M. Meyer, eds. *Methods of critical discourse analysis*. London & Thousand Oaks, CA: Sage, pp. 162-186.

Fairclough, N., 2005. Critical discourse analysis on trans-disciplinary research on social change: transition, re-scaling, poverty and social inclusion. *Lodz Papers in Pragmatics*, 1, 37-58.

Fairclough, N., 2005a. Critical discourse analysis. *Marges Linguistiques*, 9, 76-94.

Fairclough, N., 2001. The dialectics of discourse. *Textus*, XIV(2), 231-242.

Fairclough, N., 2001a. *Language and power* 2nd ed., England: Longman.

Fairclough, N., 1999. Linguistic and intertexutal analysis within discourse analysis. In A. Jaworski & N. Coupland, eds. *The discourse reader (1999)*. London & New York: Routledge, pp. 185-209.

Fairclough, N., 1996. Technologisation of discourse. In C. R. Caldas-Coulthard & M. Coulthard, eds. *Texts and practices: Readings in critical discourse analysis*. London & New York: Routledge, pp. 71-83.

Fairclough, N., 1995. *Critical discourse analysis: The critical study of language*, London: Longman.

Fairclough, N., 1993. Critical discourse analysis and the marketisation of public discourse: The universities. *Discourse Society*, 2(2), 133-168.

Fairclough, N. & Wodak, R., 1997. Critical discourse analysis. In T. A. van Dijk, ed. *Discourse as social interaction (Discourse studies: A multidisciplinary introduction)*. London, Thousand Oaks & New Delhi: Sage, pp. 258-284.

Fallows, D., 2005. Search engine users. *Pew Internet and American Life Project*. Available at: www.pewinternet.org [Accessed May 30, 2010].

Farrar, D., 2009. Why is National taking the heat for a problem they did not cause? *Kiwiblog*. Available at: http://www.kiwiblog.co.nz/2009/02/why_is_national_taking_the_heat_for_a_problem_they_did_not_cause.html [Accessed May 15, 2010].

Fenton, N., 2007. Contesting global capital, new media, solidarity, and the role of a social imaginary. In B. Cammaerts & N. Carpentier, eds. *Reclaiming the media: Communication rights and democratic media roles*. Bristol & Chicago: Intellect, pp. 225-242.

Fernback, J., 1997. The individual within the collective: Virtual ideology and the realisation of collective principles. In S. Jones, ed. *Virtual culture: Identity and communication in cybersociety*. London: Sage Publications.

Fischer-Hübner, S., 2000. Privacy and security at risk in the global information society. In D. Thomas & B. D. Loader, eds. *Cybercrime: Law enforcement, security and surveillance in the information age*. London and New York: Routledge.

Fitzgerald, B., 2010. Internet censorship remains part of Conroy's agenda. *The Australian*. Available at: http://www.theaustralian.com.au/news/opinion/internet-censorship-remains-part-of-conroys-agenda/story-e6frg6zo-1225863648749 [Accessed May 26, 2010].

Flew, T. & McElhinney, S., 2002. Globalisation and the structure of new media industries. In L. A. Lievrouw & S. Livingstone, eds. *The handbook of new media: Social shaping and consequences of ICTs*. Thousand Oaks, London & New Delhi: Sage Publications, pp. 304-319.

Flower, W., 2009. Minister Stephen Conroy slams 'juvenile' hack attack. *Herald Sun*. Available at: http://www.heraldsun.com.au/news/national/minister-stephen-conroy-slams-juvenile-hack-attack/story-e6frf7l6-1225771252907 [Accessed May 30, 2010].

Flynn, L., 2009. Our views on mandatory ISP filtering. *Official Google Australia Blog*. Available at: http://google-au.blogspot.com/2009/12/our-views-on-mandatory-isp-filtering.html [Accessed May 26, 2010].

Forsyth, D.R., 1983. *An introduction to group dynamics*, Monterey, California: Brooks/Cole.

Foucault, M., 1980. *Power/knowledge*, New York: Pantheon.

Fraley, T., 2007. The revolution will be televised: Free speech TV, democratic communication and the public sphere. In R. Butsch, ed. *Media and public spheres*. Hampshire & New York: Palgrave MacMillan, pp. 175-184.

Francis, C., 2009. Stephen Fry rails against NZ internet law. *Stuff*. Available at: http://www.stuff.co.nz/technology/1404653 [Accessed May 13, 2010].

Fraser, N., 2005. Transnationalizing the public sphere. Available at: http://www.republicart.net/disc/publicum/fraserol_en.pdf [Accessed May 13, 2010].

Fraser, N., 1995. Politics, culture, and the public sphere: Towards a postmodern conception. In L. Nicholson & S. Seidman, eds. *Social postmodernism: Beyond identity politics*. Cambridge, MA & London, England: Cambridge University Press, pp. 287-314.

Fraser, N., 1992. Rethinking the public sphere: A contribution to the critique of actually existing democracy. In C. Calhoun, ed. *Habermas and the public sphere*. Cambridge and London: MIT Press.

Free anonymising browser debuts, 2006. *BBC*. Available at: http://news.bbc.co.uk/2/hi/technology/5363230.stm [Accessed May 7, 2010].

Freeman, J., 1970. The tyranny of structurelessness. Available at: http://www.jofreeman.com/joreen/tyranny.htm [Accessed May 13, 2010].

Friedland, L.A. et al., 2007. The local public sphere as a networked space. In R. Butsch, ed. *Media and public spheres*. Hampshire & New York: Palgrave MacMillan.

Froomkin, A.M., 2004. Technologies for democracy. In P. M. Shane, ed. *Democracy online: The prospects for political renewal through the Internet*. London and New York: Routledge.

Fry, S., 2009. Stephen Fry's #blackout tweet. *Twitter*. Available at: http://twitter.com/stephenfry/status/1213914907 [Accessed May 13, 2010].

Fry, S., 2009a. Stepehen Fry's #blackout tweet #2. *Twitter*. Available at: http://twitter.com/stephenfry/status/1213907407 [Accessed May 13, 2010].

Fung, A.Y. & Kedl, K.D., 2000. Representative publics, political discourses, and the Internet: A case study of a degenerated public sphere in a Chinese online community. *World Communication*, (29(4)), 69-84.

Furnell, S. & Warren, M., 1999. Computer hacking and cyberterrorism: The real threats in the new millennium. *Computers & Security*, 18(28-34).

Gaiman, N., 2009. Neil Gaiman's #blackout tweet. *Twitter*. Available at: http://twitter.com/neilhimself/status/1227384726 [Accessed May 13, 2010].

Gallo, J., 2003. Online oppositional communities as discursive counterpublics.

Gandy Jr., O.H., 2002. The real digital divide: Citizens versus consumers. In L. A. Lievrouw & S. Livingstone, eds. *The handbook of new media: Social shaping and consequences of ICTs*. London: Sage Publications, pp. 448-460.

Garcelon, M., 2006. The 'Indymedia' experiment: The Internet as movement facilitator against institutional control. *Convergence: The International Journal of Research Into New Media Technologies*, 12(1), 55-82.

Garnham, N., 1992. The Media and the public sphere. In C. Calhoun, ed. *Habermas and the public sphere*. Cambridge & London: The MIT Press, pp. 359-376.

Garnham, N., 1990. The Media and the public sphere. In N. Garnham, ed. *Capitalism and communication*. London: Sage.

Garnham, N., 1986. The Media and the public sphere. In O. Boyd-Barrett & C. Newbold, eds. *Approaches to media: A reader (1995)*. London, New York, Sydney & Auckland: Arnold, pp. 245-251.

Garrett, R.K., 2006. Protest in an information society: A review of literature on social movements and new ICTs. Available at: http://www-personal.umich.edu/~garrettk/Garrett-ProtestInfoSociety.pdf [Accessed May 30, 2010].

Garrido, M. & Halavais, A., 2003. Mapping networks of support for the Zapatista movement: Applying social-network analysis to study contemporary social movements. In M. McCaughey & M. D. Ayers, eds. *Cyberactivism: Online*

activism in theory and practice. London & New York: Routledge, pp. 165-184.

Gastil, R., 1985. The past, present, and future of democracy. *Journal of International Affairs*, (38 (Spring)), 161-179.

Gee, J.P., 1999. Mind and society: A response to Derek Edwards' 'emotion discourse'. *Culture and Psychology*, 5(3), 305-312.

Gehring, V.V., 2004. Do hackers provide a public service? In V. V. Gehring, ed. *The Internet in public life*. Maryland: Rowman & Littlefield Publishers Inc., pp. 43-56.

Gerbner, G., 1969. Toward 'cultural indicators': The analysis of mass mediated public message systems. In O. Boyd-Barrett & C. Newbold, eds. *Approaches to media: A reader (1995)*. London, New York, Sydney & Auckland: Arnold, pp. 144-152.

GetUp! *GetUp!* Available at: http://www.getup.org.au/ [Accessed May 26, 2010].

Giddens, A., 1991. Modernity and self-identity: Tribulations of the self. In A. Jaworski & N. Coupland, eds. *The discourse reader (1999)*. London & New York: Routledge, pp. 415-427.

Gill, A.M. & Whedbee, K., 1997. Rhetoric. In T. A. van Dijk, ed. *Discourse as social interaction (Discourse studies: A multidisciplinary introduction)*. London, Thousand Oaks & New Delhi: Sage, pp. 157-184.

Gimmler, A., 2001. Deliberative democracy, the public sphere and the Internet. *Philosophy & Social Criticism*, 27(4), 21-39.

Giroux, H.A., 2000. Counter-public spheres and the role of educators as public intellectuals: Paulo Friere's cultural politics. In M. Hill & W. Montag, eds. *Masses, classes and the public sphere*. London & New York: Verso, pp. 251-268.

Gitlin, T., 1990. *The Whole World is Watching: Mass Media and the Making and Unmaking of the New Left*, Berkeley, CA: University of California Press.

Gitlin, T., 1978. Media sociology: The dominant paradigm. In O. Boyd-Barrett & C. Newbold, eds. *Approaches to media: A reader (1995)*. London, New York, Sydney & Auckland: Arnold, pp. 21-32.

Glasser, T.L. & Craft, S., 1998. Public journalism and the search for democratic ideals. In T. Liebes & J. Curren, eds. *Media, ritual & identity*. London & New York: Routledge, pp. 203-218.

Globescan Incorporated / BBC World Service, 2010. *Global Poll on Internet Access*, Available at: http://globescan.com/news_archives/bbc2010_internet/ [Accessed May 6, 2010].

Goffman, E., 1976. On face-work: An analysis of ritual elements in social interaction. In A. Jaworski & N. Coupland, eds. *The discourse reader (1999)*. London & New York: Routledge, pp. 306-320.

Goldhaber, M.H., 1997. The attention economy: The natural economy and the Internet. *First Monday*, (2(4)). Available at: http://www.firstmonday.dk/issues/issue2_4/goldhaber/ [Accessed May 30, 2010].

Golding, P., 2004. Foreword. In P. N. Thomas & Z. Nain, eds. *Who owns the media? Global trends and local resistances*. Penang, London and New York: Southbound, Zed Books.

Golding, P., 1995. The mass media and the public sphere: The crisis of information in the 'information society'. In S. Edgell, S. Walklate, & G. Williams, eds. *Debating the future of the public sphere*. Aldershot & Brookfield: Avebury, pp. 25-40.

Golding, P. & Murdock, G., 2000. Culture, communications, and political economy. In J. Curran & M. Gurevitch, eds. *Mass media and society*. London, New York: Arnold, Oxford University Press.

Gomez, J., 2004. Dumbing down democracy: Trends in Internet regulation, surveillance, and control in Asia. *Pacific Journalism Review*, 10(2), 130-150.

Gompert, D., 1988. National security in the information age. *Naval War College Review*, 51(4), 22-41.

Gould, C.C., 1996. Diversity and democracy: Representing differences. In S. Benhabib, ed. *Democracy and difference: Contesting the boundaries of the political*. Princeton, NJ: Princeton University Press, pp. 171-186.

Government websites hacked by Anonymous over censorship, 2010. *News.com.au*. Available at: http://www.news.com.au/technology/government-websites-hacked-by-anonymous-over-censorship/story-e6frfro0-1225828788264 [Accessed August 18, 2010].

Graber, D., 1992. *Public sector communication: How organisations manage information*, Washington, D.C.: Congressional Quarterly.

Grabosky, P. & Smith, R., 2000. Telecommunication fraud in the digital age. In D. Thomas & B. D. Loader, eds. *Cybercrime: Law enforcement, security and surveillance in the information age*. London and New York: Routledge.

Grabowsky, P., Smith, R.G. & Dempsey, G., 2001. *Electronic theft: Unlawful acquisition in cyberspace*, Cambridge: Cambridge University Press.

Graham, T., 2002. *Deliberating in online forums*. Amsterdam School of Communications.

Granick, J.S. et al., 2003. Sentencing guidelines for United States courts. Available at: http://cyberlaw.stanford.edu/about/cases/1030%20Comments%202-1903.pdf.

Greene, T.C., 2001. Will cDc privacy app Peekabooty put users at risk? *The Register*. Available at: http://www.theregister.co.uk/2001/07/19/will_cdc_privacy_app_peekabooty/ [Accessed May 8, 2010].

Greenleaf, G., 2003. An endnote of regulating cyberspace: Architecture vs. law? In D. S. Wall, ed. *Cyberspace crime*. Aldershot & Burlington: Ashgate.

Groups/People joining the Internet Blackout, 2009. *Creative Freedom Foundation*. Available at: http://creativefreedom.org.nz/forum/topic.php?id=103&page=1 [Accessed May 14, 2010].

Guidry, J.A., Kennedy, M.D. & Zald, M.N., 2000. Globalisations and social movements. In J. A. Guidry, M. D. Kennedy, & M. N. Zald, eds. *Globalisations and social movements: Culture, power and the transnational public sphere*. Ann Arbor: The University of Michigan Press, pp. 1-32.

Gurak, L.J. & Logie, J., 2003. Internet protests, from text to web. In M. McCaughey & M. D. Ayers, eds. *Cyberactivism: Online activism in theory and practice*. London & New York: Routledge, pp. 25-46.

Habermas, J., 2006. Political communication in media society: Does democracy still enjoy an epistemic dimension? The impact of normative theory on empirical research. *Communication Theory*, 16, 411-426.

Habermas, J., 2002. Civil society and the political public sphere. In C. Calhoun et al., eds. *Contemporary sociological theory*. Malden, MA: Blackwell, pp. 358-76.

Habermas, J., 1996. *Between facts and norms*, London: Polity Press.

Habermas, J., 1996a. Three normative models of democracy. In S. Benhabib, ed. *Democracy & difference: Contesting the boundaries of the political*. Princeton, NJ: Princeton University Press, pp. 21-30.

Habermas, J., 1992. Further reflections on the public sphere. In C. Calhoun, ed. *Habermas and the public sphere*. Cambridge: MIT Press.

Habermas, J., 1989. *The structural transformation of the public sphere*, Massachusetts: MIT Press.

Habermas, J., 1987. *The theory of communicative action: The critique of functionalist reason*, Cambridge: Polity Press.

Hacker, K.L. & J. van Dijk, 2000. What is digital democracy? In K. L. Hacker & J. van Dijk, eds. *Digital democracy: Issues of theory and practice*. London,

Thousand Oaks & New Delhi: Sage Publications, pp. 1-9.

Hackers 'titstorm' the PM and Parliament House, 2010. *The Australian*. Available at: http://www.theaustralian.com.au/news/nation/hackers-titstorm-the-pm-and-parliament-house/story-e6frg6nf-1225828956252 [Accessed August 18, 2010].

Hackers disrupt Australian Government web sites, 2010. *American Broadcasting Company (ABC)*. Available at: http://abcnews.go.com/Technology/wireStory?id=9799170 [Accessed August 18, 2010].

Hackers hit New Zealand Herald website, 2007. *Stuff.co.nz*. Available at: http://www.stuff.co.nz/technology/18026 [Accessed May 2, 2010].

Hackers protesting against a proposed internet filter that targets pornography shut down Federal Government website, 2010. *Herald Sun*. Available at: http://www.heraldsun.com.au/news/hackers-protesting-against-a-proposed-internet-filter-that-targets-pornography-shut-down-federal-government-website/story-e6frf7jo-1225828766740 [Accessed August 18, 2010].

Hacktivismo. *Wikipedia*. Available at: http://en.wikipedia.org/wiki/Hacktivismo [Accessed May 7, 2010].

Hacktivismo FAQ. *Cult of the Dead Cow*. Available at: http://www.cultdeadcow.com/cDc_files/HacktivismoFAQ.html [Accessed May 7, 2010].

Hacktivismo releases Torpark for anonymous, portable web browsing, 2006. *Cult of the Dead Cow*. Available at: http://w3.cultdeadcow.com/cms/2006/09/hacktivismo-rel.html [Accessed May 7, 2010].

Hacktivismo: Board of Advisors. *Hacktivismo*. Available at: http://www.hacktivismo.com/about/index.php [Accessed May 7, 2010].

Hacktivismo: HESSLA. *Hacktivismo*. Available at: http://www.hacktivismo.com/about/hessla.php [Accessed May 7, 2010].

Hacktivismo: News. *Hacktivismo*. Available at: http://www.hacktivismo.com/news/ [Accessed May 7, 2010].

Hafner, K. & Markoff, J., 1991. *Cyberpunk: Outlaws and hackers on the computer frontiers*, New York: Simon and Schuster.

Hague, B. & Loader, B., 1999. *Digital democracy and decision making in the information age*, London and New York: Routledge.

Halbert, D., 1997. Discourses of danger and the computer hacker. *The Information Society*, 13, 361-374.

Hall, A., 2010. Clinton speech boosts anti-filter campaign. *ABC News*. Available at: http://www.abc.net.au/news/stories/2010/01/22/2799369.htm [Accessed May 26, 2010].

Hall, S., 1981. Encoding/decoding. In S. Hall et al., eds. *Culture, media, language*. London: Hutchison.

Halliday, M., 1994. *An introduction to functional grammar* 2nd ed., London: Edward Arnold.

Halliday, M., 1978. *Language as social semiotic*, London: Edward Arnold.

Halliday, M. & Hasaan, R., 1985. *Language, context and text* 2nd ed., Oxford: Oxford University Press.

Hancock, B., 1998. Security views. *Computers and Security*, 17(1), 5.

Hands, J., 2007. Bewteen agonistic and deliberative politics: Towards a radical e-democracy. In L. Dahlberg & E. Siapera, eds. *Radical democracy and the Internet*. Hampshire & New York: Palgrave MacMillan, pp. 89-107.

Hannemyr, G., 1998. Technology & pleasure: The art and craft of hacking. Available at: http://hannemyr.com/essay/sj98.html [Accessed May 26, 2010].

Hannemyr, G., 1997. Technology & pleasure: Hacking considered constructive. Available at: http://hannemyr.com/essay/oks97.html [Accessed May 26, 2010].

Hardt, M., 2000. The withering of civil society. In M. Hill & W. Montag, eds. *Masses, classes and the public sphere*. London & New York: Verso, pp. 158-178.

Hargittai, E., 2004. The changing online landscape: From free-for-all to commercial gatekeeping. In P. Day & D. Schuler, eds. *Community practice in the network society: Local actions/global interaction*. New York: Routledge, pp. 66-76.

Harju, A., 2007. Citizen participation and local public spheres: An agency and identity focused approach to the Tampere Postal Services conflict. In B. Cammaerts & N. Carpentier, eds. *Reclaiming the media: Communication rights and democratic media roles*. Bristol & Chicago: Intellect, pp. 92-106.

Harmon, A., 2004. Politics of the Web: Meet, greet, segregate, meet again. *New York Times*.

Harris, S., 2001. Being politically impolite: Extending politeness theory to adversarial political discourse. *Discourse Society*, 12(4), 451-472.

Hearn, L., 2010. Study casts doubt over net filter support. *The Sydney Morning*

Herald. Available at: http://www.smh.com.au/technology/technology-news/study-casts-doubt-over-net-filter-support-20100512-uvo0.html [Accessed May 26, 2010].

Herman, E.S. & McChesney, R.W., 1997. *The global media: The new missionaries of global capitalism*, London and Washington: Cassell.

Herman, E.S. & Chomsky, N., 1988. *Manufacturing consent: The political economy of the mass media*, New York: Pantheon Books.

Hernandes-Flores, N., 1999. Politeness ideology in Spanish colloquial conversation: The case of advice. *Pragmatics*, (9), 37-49.

HESSLA: Hacktivismo Enhanced-Source Software License Agreement. *Wikipedia*. Available at: http://en.wikipedia.org/wiki/Hacktivismo_Enhanced-Source_Software_License_Agreement [Accessed May 7, 2010].

Hill, K.A. & Hughes, J.E., 1998. *Cyberpolitics: Citizen activism in the age of the Internet*, Lanham & Oxford: Rowman & Littlefield Publishers Inc.

Hill, M., 2000. Of multitudes and moral sympathy: E.P. Thompson, Althusser, and Adam Smith. In M. Hill & W. Montag, eds. *Masses, classes and the public sphere*. London & New York: Verso, pp. 202-225.

Hill, M. & Montag, W., 2000. Introduction: What was, what is, the public sphere? Post Cold-War reflections. In M. Hill & W. Montag, eds. *Masses, classes and the public sphere*. London & New York: Verso, pp. 1-12.

Himanen, P., 2001. *The hacker ethic : A radical approach to the philosophy of business*, New York: Random House.

Himma, K.E., 2007. Hacking as politically motivated digital disobedience: Is hacktivism morally justified? In K. E. Himma, ed. *Readings on Internet security: Hacking, counterhacking and other moral issues*. Massachusetts: Jones & Bartlett, pp. 73-98.

Hindman, M., 2007. "Open-source politics" reconsidered: Emerging patterns in online political participation. In V. Mayer-Schonberger & D. Lazer, eds. *Governance and information technology: From electronic government to information government*. Cambridge, MA., & London: The MIT Press, pp. 183-207.

Ho, C., 2010. Titstorm still flooding govt. *ZDNet*. Available at: http://www.zdnet.com.au/titstorm-still-flooding-govt-339300977.htm [Accessed August 18, 2010].

Hoar, P. & Hope, W., 2002. The Internet, the public sphere and the "digital divide" in New Zealand. *Journal of International Communication*, 8(2), 64-88.

Hoggett, P. & Thompson, S., 2002. Toward a democracy of the emotions.

Constellations, (9(1)), 106-126.

Hollinger, R. & Lanza-Kaduce, L., 1988. The process of criminalisation: The case of computer crime laws. *Criminology*, 26, 101-126.

Holmes, D., 1997. Introduction: virtual politics - Identity and communication in cyberspace. In D. Holmes, ed. *Virtual politics: Identity and communication in cyberspace*. Thousand Oaks: Sage Publications, pp. 1-25.

Horrigan, J., 2001. Online communities: Networks that nurture long-distance relationships and local ties. *Pew Internet and American Life Project*. Available at: http://pewinternet.org/pdfs/PIP_Communities_Report.pdf [Accessed May 26, 2010].

Horrigan, J., Garrett, K. & Resnick, K., 2004. *The Internet and democratic debate*, Washington, DC: Pew Internet & American Life Project.

How Copyright is Harming Creativity (CFF). *Creative Freedom Foundation*. Available at: http://creativefreedom.org.nz/creativity.html [Accessed May 13, 2010].

How to permanently delete your Facebook account. *Facebook*. Available at: http://www.facebook.com/group.php?gid=16929680703 [Accessed May 16, 2010].

Hunter, D., 2004. ICANN and electronic democratic deficit. In *Democracy online: The prospects for political renewal through the Internet*. Routledge: London & New York, pp. 141-152.

Hurwitz, R., 2003. Who needs politics? Who needs people? The ironies of democracy in cyberspace. In H. Jenkins, D. Thorburn, & B. Seawell, eds. *Democracy and new media*. Cambrdige: MIT Press, pp. 101-111.

IHTFP Hack Gallery. *IHTFP Hack Gallery*. Available at: http://hacks.mit.edu/Hacks/ [Accessed April 16, 2010].

In the Press - Periodicals. *Cult of the Dead Cow*. Available at: http://w3.cultdeadcow.com/cms/press.html [Accessed May 13, 2010].

Internet Censorship Australia. *YouTube*. Available at: http://www.youtube.com/v/THPscN652-0 [Accessed May 31, 2010].

Internet restrictions curtail human rights, says US, 2010. *BBC*. Available at: http://news.bbc.co.uk/2/hi/americas/8563084.stm [Accessed May 7, 2010].

Introna, L.D. & Nissenbaum, H., 2000. Shaping the Web: Why the politics of search engines matters. *Information Society*, 16(3), 169-185.

Jacobs, C., 2010. Vigilantism is bad for the cause. *Electronic Frontiers Australia*. Available at: http://www.efa.org.au/2010/02/10/vigilantism-is-bad-for-the-

cause/ [Accessed August 23, 2010].

Jacobs, C., 2008. EFA says filtering trial a failure. *Electronic Frontiers Australia*. Available at: http://www.efa.org.au/2008/07/31/efa-says-filtering-trial-a-failure/ [Accessed May 26, 2010].

Jäger, S. & Maier, F., 2009. Theoretical and methodological aspects of Foucauldian critical discourse analysis and dispositive analysis. In R. Wodak & M. Meyer, eds. *Methods of critical discourse analysis*. London & Thousand Oaks, CA: Sage, pp. 34-61.

Jankowski, N.W., 2002. Creating community with media: History, theories and scientific investigations. In L. A. Lievrouw & S. Livingstone, eds. *The handbook of ICT: Social shaping and consequences of ICTs*. London: Sage Publications.

Jaworski, A. & Coupland, N., 1999. Introduction: Perspectives on discourse analysis. In A. Jaworski & N. Coupland, eds. *The discourse reader (1999)*. London & New York: Routledge, pp. 1-39.

Jenkins, H. & Thorburn, D., 2003a. *Democracy and new media*, Cambridge, Massachussets: MIT Press.

Jenkins, H. & Thorburn, D., 2003b. Introduction: The Digital Revolution, The Informed Citizen and the Culture of Democracy. In H. Jenkins, D. Thorburn, & B. Seawell, eds. *Democracy and New Media*. Cambridge: MIT Press, pp. 1-17.

Johnson, B., 2009. The lights are going out all over Twitter. *The Guardian*. Available at: http://www.guardian.co.uk/technology/2009/feb/17/internet-newzealand [Accessed May 13, 2010].

Johnson, D., 1994. Crime, abuse and hacker ethics. *EDUCOM Review*, 29(5), 40-50.

Johnston, C., 2010. Botnets increasingly wielded for ideological uses. *Ars Technica*. Available at: http://arstechnica.com/security/news/2010/02/botnets-increasingly-wielded-for-ideological-uses.ars [Accessed August 14, 2010].

Join the Internet Blackout - Protest Against Guilt Upon Accusation Laws in NZ (CFF). *Creative Freedom Foundation*. Available at: http://creativefreedom.org.nz/blackout.html [Accessed May 13, 2010].

Jones, S., 1998. *CyberSociety 2.0: Revisiting computer-mediated communication and community*, Thousand Oaks: Sage Publications.

Jones, S., 1997. The Internet and its social landscape. In S. G. Jones, ed. *Virtual culture: Identity and communication in cyberspace*. London: Sage Publications.

de Jong, W., Shaw, M. & Stammers, N., 2005. Introduction. In W. D. Jong, M. Shaw, & N. Stammers, eds. *Global activism, global media*. London & Ann Arbor: Pluto Press, pp. 1-14.

Jordan, T., 2008. *Hacking.* Cambridge & Malden, MA., Polity Press.

Jordan, T., 2007. Online direct action: Hacktivism and radical democracy. In L. Dahlberg & E. Siapera, eds. *Radical democracy and the Internet*. Hampshire & New York: Palgrave MacMillan, pp. 73-88.

Jordan, T., 1999. *Cyberpower: The culture and politics of cyberspace and the Internet*, London & New York: Routledge.

Jordan, T. & Taylor, P.A., 2004. *Hacktivism and cyberwars: Rebels with a cause?*, London and New York: Routledge.

Jordan, T. & Taylor, P., 1998. A sociology of hackers. *The Sociological Review*, 46(4), 757-780.

Juris, J.S., 2005. The new digital media and activist networking within anti-corporate globalization movements. *The ANNALS of the American Academy of Political and Social Science*, 597, 189-208.

Kahn, R. & Kellner, D., 2006. Internet subcultures and oppositional politics. Available at: http://www.gseis.ucla.edu/faculty/kellner/kellner.html [Accessed May 26, 2010].

Kahn, R. & Kellner, D., 2006b. Resisting globalisation. Available at: http://richardkahn.org/flash.html [Accessed May 26, 2010].

Kahn, R. & Kellner, D., 2005. Oppositional politics and the internet: A critical/reconstructive approach. Available at: http://www.gseis.ucla.edu/faculty/kellner/kellner.html [Accessed May 26, 2010].

Kahn, R. & Kellner, D., 2004. New media and internet activism: From the 'Battle of Seattle' to blogging. *New Media & Society*, 6(1), 87-95.

Katz, E. & Lazarsfeld, P.F., 1955. Between media and mass/The part played by people/The two-step flow of communication. In O. Boyd-Barrett & C. Newbold, eds. *Approaches to media: A reader (1995)*. London, New York, Sydney & Auckland: Arnold, pp. 124-134.

Kavada, A., 2009. Collective action and the social web: Comparing the architecture of Avaaz.org and Openesf.net. In N. Carpentier et al., eds. *Communicative Approaches to Politics and Ethics in Europe*. Estonia: Tartu University Press, pp. 129-140.

Keall, C., 2009. Section 92A to be scrapped. *The National Business Review*. Available at: http://www.nbr.co.nz/article/section-92a-be-scrapped-89121

[Accessed May 13, 2010].

Keane, J., 2000. Structural transformations of the public sphere. In K. L. Hacker & J. van Dijk, eds. *Digital democracy: Issues of theory and practice*. London, Thousand Oaks & New Delhi: Sage Publications, pp. 70-89.

Keane, J., 1993. Democracy and media: Without foundations. In O. Boyd-Barrett & C. Newbold, eds. *Approaches to media: A reader (1995)*. London, New York, Sydney & Auckland: Arnold, pp. 263-268.

Keck, M. & Sikkink, K., 2000. Historical precursors to modern transnational social movements. In J. A. Guidry, M. D. Kennedy, & M. N. Zald, eds. *Globalisations and social movements: Culture, power and the transnational public sphere*. Ann Arbor: University of Michigan Press, pp. 35-53.

Kedzie, C.R., 1995. A brave new world or a new world order? In S. Kiesler, ed. *Research outposts on the information highway*. Hillsdale, New Jersey: Erlbaum Associates.

Keen, A., 2007. *The cult of the amateur: How today's Internet is killing our culture and assaulting our economy*, London & Boston: Nicholas Brealey Publishing.

Kellner, D., 2006. Globalization, technopolitics and revolution. Available at: http://www.gseis.ucla.edu/aculty/kellner/kellner.html [Accessed May 26, 2010].

Kellner, D., 2004. The media and the crises of democracy in the age of Bush-2. *Communication and critical/cultural studies*, (1(1)), 29-58.

Kellner, D., 2000. Habermas, the public sphere, and democracy: A critical intervention. Available at: http://www.gseis.ucla.edu/faculty/kellner/kellner.html [Accessed May 26, 2010].

Kellner, D., 1997. Intellectuals, the new public spheres, and techno-politics. Available at: http://www.gseis.ucla.edu/faculty/kellner/kellner.html [Accessed May 26, 2010].

Kellner, D., 1995. Intellectuals and new technologies. Available at: http://www.gseis.ucla.edu/faculty/kellner/kellner.html [Accessed May 26, 2010].

Kelty, C.M., 2004. Culture's open sources: Software, copyright and cultural critique. *Anthropological Quarterly*, 77(3), 499-506

Kelty, C.M., 2002. Hau to do things with words. Available at: http://kelty.org/or/ [Accessed May 4, 2010].

Kerner, S., 2010. Ubuntu claims 12 million users as Lucid Linux desktop nears.

Linux Planet. Available at: http://www.linuxplanet.com/linuxplanet/reports/7032/1/ [Accessed April 16, 2010].

Kevin Rudd's website hacked over internet censorship, 2009. *News.com.au*. Available at: http://www.news.com.au/technology/kevin-rudds-website-hacked-over-internet-censorship/story-e6frfro0-1225771256672 [Accessed May 30, 2010].

Khleif, R.B., 2001. Hacktivists or cyberpunks? A contextualisation of differential representations.

Kidd, D., 2003. Indymedia.org: A new communicative commons. In M. McCaughey & M. D. Ayers, eds. *Cyberactivism: Online activism in theory and practice*. London & New York: Routledge, pp. 47-70.

Kidd, D., 2002. Which would you rather: Seattle or Porto Allegre? In *Our Media, Not Theirs*. Barcelona.

Kiesler, S., Siegel, J. & McGuire, T.W., 1984. Social psychological aspects of computer-mediated communication. *American Psychologist*, (10 (October)), 1123-43.

Kirkpatrick, G., 2004. *Critical technology: A social theory of personal computing*, Aldershot and Burlington: Ashgate Publishing.

Kiwicon FAQ. *Kiwicon*. Available at: https://www.kiwicon.org/faq/#q15 [Accessed May 9, 2010].

Kiwicon: Wikipedia. *Wikipedia*. Available at: http://en.wikipedia.org/wiki/Kiwicon [Accessed April 16, 2010].

Klein, N., 2002. The vision thing: Were the DC and Seattle protests unfocused, or are critics missing the point? In B. H. Shephard & R. Hayduk, eds. *From ACT UP to the WTO : Urban protest and community building in the era of globalization*. London: Verso.

Kling, R., 1996. Hopes and horrors: Technological utopianism and anti-utopianism in narratives of computerisation. In R. Kling, ed. *Computerisation and controversy*. Boston, MA: Academic Press, pp. 40-58.

Kohut, A., 2008. The Internet gains in politics. *Pew Internet and American Life Project*. Available at: http://www.pewinternet.org/Reports/2008/The-Internet-Gains-in-Politics.aspx [Accessed May 6, 2010].

Kovacich, G., 1997. Information warfare and the information systems security professional. *Computers and security*, 16, 14-24.

Kowal, D., 2002. Digitising and globalising indigenous voices: The Zapatista movement. In G. Elmer, ed. *Critical perspectives on the Internet*. Lanham,

Maryland: Rowman & Littlefield, pp. 105-126.

Kramarae, C., 1999. The language and nature of the Internet: The meaning of global. *New Media and Society*, (1(1)).

Kratt, K., 2008. Goolag Scanner released! *Cult of the Dead Cow*. Available at: http://w3.cultdeadcow.com/cms/2008/02/goolag-scanner.html [Accessed May 7, 2010].

Kratt, K., 2006. cDc launches global campaign against Google. *Cult of the Dead Cow*. Available at: http://w3.cultdeadcow.com/cms/2006/02/cdc-launches-gl.html [Accessed May 7, 2010].

Kratt, K., 2002. Camera/Shy announcement. *Cult of the Dead Cow*. Available at: http://w3.cultdeadcow.com/cms/2002/07/camerashy-annou.html [Accessed May 7, 2010].

Kravets, D., 2010. Anonymous unfurls 'Operation Titstorm'. *Wired*. Available at: http://www.wired.com/threatlevel/2010/02/anonymous-unfurls-operation-titstorm/ [Accessed August 18, 2010].

Kress, G., Leite-Garcia, R. & van Leeuwen, T., 1997. Discourse semiotics. In T. A. van Dijk, ed. *Discourse as social interaction (Discourse studies: A multidisciplinary introduction)*. London, Thousand Oaks & New Delhi: Sage, pp. 257-291.

Kuttner, R., 1999. *Everything for sale: The virtues and limits of markets*, Chicago: University of Chicago Press.

Laclau, E., 1996. *Emancipation(s)*, London: Verso.

Laclau, E., 1990. *New reflections on the revolution of our times*, London: Verso.

Laclau, E. & Mouffe, C., 1985. *Hegemony & socialist strategy: Towards a radical democratic politics*, London: Verso.

Langman, L., 2005. From virtual public spheres to global justice: A critical theory of internetworked social movements. *Sociological Theory*, 23: 1, 42-74.

Laporte, L., 2009. Leo Laporte's #blackout tweet. *Twitter*. Available at: http://twitter.com/LeoLaporte/status/1225349092 [Accessed May 13, 2010].

Lasswell, H.D., 1964. The structure and function of communication in society. In O. Boyd-Barrett & C. Newbold, eds. *Approaches to media: A reader (1995)*. London, New York, Sydney & Auckland: Arnold, pp. 93-94.

Lawrence, S. & Giles, C.L., 1999. Accessibility of information on the Web. *Nature*, (400), 107-109.

Lax, S., 2004. The Internet and democracy. In D. Gauntlett & R. Horsley, eds. *Web*

studies. New York: Oxford University Press, pp. 217-229.

Lazar, A. & Lazar, M.M., 2004. The discourse of the New World Order: 'Out-casting' the double face of threat. *Discourse and Society*, 15(2-3), 232-242.

Lee, B., 1992. Textuality, mediation, and public discourse. In C. Calhoun, ed. *Habermas and the public sphere*. Cambridge & London: The MIT Press, pp. 402-420.

Lee, K., 2005. The momentum of control and autonomy: A local scene of peer-to-peer music-sharing technology. *Media, Culture & Society*, 27(5), 799-809.

Van Leeuwen, T. 2007. Legitimation in discourse and communication. *Discourse and Communication*, 1(1), 91-112.

van Leeuwen, T., 2009. Discourse as the recontextualisation of social practice: A guide. In R. Wodak & M. Meyer, eds. *Methods of critical discourse analysis*. London & Thousand Oaks, CA: Sage, pp. 144-161.

van Leeuwen, T., 1996. The representation of social actors. In C. R. Caldas-Coulthard & M. Coulthard, eds. *Texts and practices: Readings in critical discourse analysis*. London & New York: Routledge, pp. 32-70.

van Leeuwen, T. & Wodak, R., 1999. Legitimising immigration: A discourse-historical approach. *Discourse Studies*, 1, 83-118.

Leitner, H., Peck, J. & Sheppard, E.S., 2007. Squaring Up to Neoliberalism. In H. Leitner, J. Peck, & E. S. Sheppard, eds. *Contesting Neoliberalism: Urban Frontiers*. New York & London: The Guildford Press, pp. 311-327.

Leitner, H., Sheppard, E.S. et al., 2007. Contesting urban futures: Decentering neoliberalism. In *Contesting neoliberalism: Urban frontiers*. New York & London: The Guildford Press, pp. 1-25.

Leizerov, S., 2000. Privacy advocacy groups versus Intel: A case study of how social movements Are tactically using the Internet to fight corporations. *Social Science Computer Review*, 18(4), 461-483.

LeMay, R., 2010. 92% of Whirlpool users against filter. Available at: http://apcmag.com/92-of-whirlpool-users-against-filter.htm [Accessed May 26, 2010].

LeMay, R., 2010a. Attacks on Conroy work better than petitions: "Anonymous". *APC magazine*. Available at: http://apcmag.com/attacks-on-conroy-work-better-than-petitions-anonymous.htm [Accessed August 16, 2010].

Lerner, D., 1968. *The passing of traditional society: Modernizing the Middle East*, New York: Free Press.

Lessig, L., 2004. *Free culture: How big media uses technology and the law to lock*

down culture and control creativity, New York: The Penguin Press.

Lessig, L., 1999. *Code: And other laws of cyberspace*, New York: Basic Books.

Leudar, I., Marsland, V. & Nekvapil, J., 2004. On membership categorisation: 'Us', 'them' and 'doing violence' in political discourse. *Discourse and Society*, 15(2-3), 243-266.

Levine, P., 2004. The Internet and civil society. In V. V. Gehring, ed. *The Internet in public life*. Maryland: Rowman & Littlefield Publishers Inc.

Levy, S., 1984. *Hackers: Heroes of the computer revolution*, Garden City and New York: Anchor Press/Doubleday.

Leyden, J., 2010. Activists unleash Operation Titstorm on Aussie.gov. *The Register*. Available at: http://www.theregister.co.uk/2010/02/10/aus_gove_ddos_protest/ [Accessed August 16, 2010].

Leyden, J., 2010a. Aussie anti-censor attacks strafe gov websites. *The Register*. Available at: http://www.theregister.co.uk/2010/02/11/oz_anti_censorship_ddos_latest/ [Accessed August 16, 2010].

Leyshon, A. et al., 2005. On the reproduction of the musical economy after the Internet. *Media, Culture & Society*, 27(2), 177-209.

Lievrouw, L.A., 2002. Determination and contingency in new media development: Diffusion of innovations and social shaping of technology perspectives. In L. A. Lievrouw & S. Livingstone, eds. *The handbook of new media: Social shaping and consequences of ICTs*. London: Sage Publications, pp. 181-199.

Lifehacker. *Lifehacker*. Available at: http://lifehacker.com/ [Accessed May 2, 2010].

Lindblom, C.E., 2001. *The market system: What it is, how it works, and what to make of it*, New Haven: Yale University Press.

Lispet, S.M., 1999. Some social requisites of democracy: Economic development and political legitimacy. *The American Political Science Review*, (53 (March)), 69-105.

Lispet, S.M., Seong, K. & Torres, J., 1993. A comparative analysis of the social requisites of democracy. *International Social Science Journal*, (136 (September)), 155-75.

Liu, A., 2004. *The laws of cool: Knowledge work and the culture of information*, Chicago and London: University of Chicago Press.

Livingstone, S., 2005. Critical debates in Internet studies: Reflections on an emerging field. In J. Curran & M. Gurevitch, eds. *Mass media & society*. London & New York: Oxford University Press & Hodder Arnold, pp. 9-28.

Locke, T., 2004. *Critical discourse analysis*, London & New York: Continuum.

Loper, D.K., 2000. *The criminology of computer hackers: A qualitative and quantitative analysis*. Doctor of Philosophy. University of Michigan, Criminology.

Louw, E., 2001. *The media and cultural production*, Thousand Oaks, London & New Delhi: Sage Publications.

Lovelock, P. & Ure, J., 2002. The new economy: Internet telecommunications and electronic commerce? In L. A. Lievrouw & S. Livingstone, eds. *The handbook of new media: Social shaping and consequences of ICTs*. Thousand Oaks, London & New Delhi: Sage Publications, pp. 350-368.

Lovink, G., 2002. *Dark fibre: Tracking critical Internet culture*, Massachusetts and London: MIT Press.

Luke, T.W., 2002. Power and political culture. In L. A. Lievrouw & S. Livingstone, eds. *The handbook of new media: Social shaping and consequences of ICTs*. Thousand Oaks, London & New Delhi: Sage Publications, pp. 518-532.

Lyotard, J., 1984. *The postmodern condition*, Minneapolis: University of Minnesota Press.

Macgilchrist, F., 2003. Positive discourse analysis: contesting dominant discourses by reframing the issues. *Critical Approaches to Discourse Analysis Across Disciplines*, 1(1), 74-94.

MacManus, R., 2009. Black out your twitter photo: NZ copyright law protest goes viral. *Read Write Web*. Available at: http://www.readwriteweb.com/archives/nz_internet_blackout.php [Accessed May 15, 2010].

Magaziner, I., 2003. Democracy and cyberspace: First principles. In H. Jenkins, D. Thorburn, & B. Seawell, eds. *Democracy and new media*. Cambridge: MIT Press, pp. 113-131.

Main, B., 2000. Information warfare and its impact on the information technology industry in New Zealand. In *National Advisory Committee on Computing Qualifications 2000*. Wellington, New Zealand. Available at: http://www.naccq.ac.nz [Accessed May 26, 2010].

Making a submission to a Parliamentary select committee. *New Zealand Parliament*. Available at: http://www.parliament.nz/en-NZ/AboutParl/HowPWorks/Procedures/4/9/e/00CLOOCMakingSubmission1-Making-a-submission-to-a-Parliamentary-select.htm [Accessed May 17,

2010].

Mamadouh, V., 2004. Internet, scale and the global grassroots: Geographies of the Indymedia network of Independent Media Centres. *Tijdschrift voor Economische en Sociale Geografie*, 95(5), 482-497.

Manion, M. & Goodrum, A., 2000. Terrorism or civil disobedience? Toward a hacktivist ethic. *Computers and Society*, (June 2000), 14-19.

Mao, L., 1994. Beyond politeness theory: "Face" revisited and renewed. *Journal of Pragmatics*, (21), 451-86.

Markoff, J. (2011). Malware Aimed at Iran Hit Five Sites, Report Says. *The New York Times*. Available at: http://www.nytimes.com/2011/02/13/science/13stuxnet.html?_r=1&scp=1&sq=Malware%20Aimed%20At%20Iran%20Hit%20Five%20Sites,%20Report%20Says&st=cse [Accessed June 1, 2011).

Marks, K., 2010a. "Operation Titstorm" hackers declare cyber war on Australia. *The Independent*. Available at: zotero://attachment/1293/ [Accessed August 18, 2010].

Marks, K., 2010b. Operation Titstorm - Hackers declare war on Aussie. *The New Zealand Herald*. Available at: http://www.nzherald.co.nz/compute/news/article.cfm?c_id=1501832&objectid=10625493 [Accessed August 16, 2010].

Marshall, M., 2004. The effects of piracy upon the music industry: A case study of bootlegging. *Media, Culture & Society*, 26(2), 163-181.

Martin, J.R., 2004. Positive discourse analysis: Solidarity and change. *Revista Canaria de Estudios Ingleses*, 49, 179-200.

Masnick, M., 2009. Sony Pictures having its best box office year ever... still blaming piracy for killing the business. *Techdirt*. Available at: http://www.techdirt.com/articles/20091117/2239296982.shtml [Accessed May 14, 2010].

Mautner, G., 2009. Checks and balances: How corpus linguistics can contribute to CDA. In R. Wodak & M. Meyer, eds. *Methods of critical discourse analysis*. London & Thousand Oaks, CA: Sage, pp. 122-143.

Mazzocco, D.W., 1994. *Networks of power*, Boston: South End Press.

McCaughey, M. & Ayers, M.D., 2003. Introduction. In M. McCaughey & M. D. Ayers, eds. *Cyberactivism: Online activism in theory and practice*. London & New York: Routledge, pp. 1-24.

McChesney, R., 2004. The political economy of international communications. In P. N. Thomas & Z. Nain, eds. *Who owns the media: Global trends and local*

resistances. Penang, London and New York: Southbound Press, Zed Books.

McChesney, R., 2004a. Making a Mountain out of a Molehill: The Sad State of Political Economy in U.S. Media Studies. In A. Calabrese & C. Sparks, eds. *Toward A Political Economy of Culture: Capitalism and Communication in the Twenty-First Century*. Lanham, Maryland: Rowman & Littlefield Publishers, Inc., pp. 41-64.

McChesney, R., 2004b. *The Problem of the media: U.S. communication politics in the 21st century*, New York: Monthly Review Press.

McChesney, R., 2002. The global restructuring of media ownership. In M. Raboy, ed. *Global media policy in the new millennium*. Luton: University of Luton Press.

McChesney, R., 2000. So much for the magic of technology and the free market. In A. Herman & T. Swiss, eds. *The World Wide Web and contemporary cultural theory*. New York: Routledge.

McChesney, R., 1999. *Rich media, poor democracy: Communications politics in dubious times*, Illinois: University of Illinois Press.

McChesney, R. & Schiller, D., 2002. *The political economy of international communications: Foundations for the emerging global debate over media ownership and regulation*, United Nations Research Institute for Social Development.

McColm, R.B., 1992. The comparative survey of freedom 1991-1992: Between two worlds. In Freedom House Survey Team, ed. *Freedom in the world: Political rights and civil liberties, 1991-1992*. New York: Freedom House.

McCourt, T. & Burkart, P., 2003. When creators, corporations and consumers collide: Napster and the development of on-line music distribution. *Media, Culture & Society*, 25, 333-350.

McInerney, D., 2000. Print-capitalism? In M. Hill, ed. *Masses, classes and the public sphere*. London & New York: Verso, pp. 179-201.

McLaughlin, L., 2004. Feminism and the political economy of transnational public space. In N. Crossley & L. M. Roberts, eds. *After Habermas: New perspectives on the public sphere*. Oxford: Blackwell Publishing.

McLean, W. (2010). Iran 'first victim of cyberwar'. *The Scotsman.* Available at: http://news.scotsman.com/world/Iran-39first-victim-of-cyberwar39.6550278.jp [Accessed June 1, 2011].

Mehra, B., Merkel, C. & Bishop, A.P., 2004. The Internet for empowerment of minority and marginalised users. *New Media & Society*, 6(6), 781-802.

Meikle, G., 2002. *Future active: Media activism and the Internet*, New York and London: Routledge.

Mendelsohn, B., 2005. Sovereignty under attack: the international society meets the Al-Quaeda network. *Review of International Studies*, (31), 45-68.

Message To The Australian Government From Anonymous, 2009. *YouTube*. Available at: http://www.youtube.com/watch?v=CEe7qhlFNs4 [Accessed May 26, 2010].

Miège, B., 2004. Capitalism and communication: A new era of society or the accentuation of long-term tendencies? In A. Calabrese & C. Sparks, eds. *Toward a political economy of culture: Capitalism and communication in the twenty-first century*. Lanham, Maryland: Rowman & Littlefield Publishers, Inc., pp. 83-94.

Miller, C., 2006. Cheated by the click of a button. *Sunday Star Times 22/01/06*, A14.

Miller, V., 2004. Stitching the Web into global capitalism. In D. Gauntlett & R. Horsley, eds. *Web studies*. London: Edward Arnold Publishers Ltd.

Montag, W., 2000. The pressure of the street: Habermas's fear of the masses. In M. Hill & W. Montag, eds. *Masses, classes and the public sphere*. London & New York: Verso, pp. 132-145.

Morris, D., 2004. Globalization and media democracy: The case of Indymedia. In D. Schuler & P. Day, eds. *Shaping the network society: The new role of civil society in cyberspace*. Cambridge: MIT Press.

Morrisett, L., 2003. Technologies of freedom? In H. Jenkins, D. Thorburn, & B. Seawell, eds. *Democracy and new media*. Cambridge: MIT Press, pp. 21-31.

Mosco, V., 2004a. Capitalism's Chernobyl? From Ground Zero to Cyberspace and Back Again. In A. Calabrese & C. Sparks, eds. *Toward A Political Economy of Culture: Capitalism and Communication in the Twenty-First Century*. Lanham, Maryland: Rowman & Littlefield Publishers, Inc., pp. 211-227.

Mosco, V., 2004b. *The digital sublime: Myth, power and cyberspace*, London & Cambridge, MA: The MIT Press.

Mosco, V., 2000. Webs of myth and power. In A. Herman & T. Swiss, eds. *The World Wide Web and contemporary cultural theory*. New York: Routledge.

Mosco, V., 1996. *The political economy of communication: Rethinking and renewal*, London and Thousand Oaks: Sage Publications.

Moses, A., 2010. Operation Titstorm: hackers bring down government websites. *The Sydney Morning Herald*. Available at: http://www.smh.com.au/technology/technology-news/operation-titstorm-hackers-bring-down-government-websites-20100210-nqku.html [Accessed August 18, 2010].

Moses, A., 2010a. Operation Titstorm hackers strike Australia. *Stuff.co.nz*. Available at: http://www.stuff.co.nz/technology/digital-living/3312167/Operation-Titstorm-hackers-strike-Australia [Accessed August 18, 2010].

Moses, A., 2009. Leaked Australian blacklist reveals banned sites. *The Sydney Morning Herald*. Available at: http://www.smh.com.au/articles/2009/03/19/1237054961100.html [Accessed May 26, 2010].

Moses, A., 2009a. Web censorship plan heads towards a dead end. *The Sydney Morning Herald*. Available at: http://www.smh.com.au/news/technology/biztech/web-censorship-plan-heads-towards-a-dead-end/2009/02/26/1235237810486.html?page=fullpage [Accessed May 26, 2010].

Moses, A., 2009b. Hacked by hoons: how attack on PM's website unraveled. *The Sydney Morning Herald*. Available at: http://www.smh.com.au/technology/security/hacked-by-hoons-how-attack-on-pms-website-unravelled-20090910-fipj.html [Accessed May 30, 2010].

Moses, A., 2009c. Rudd hackers escalate threats against .gov.au websites. *The Sydney Morning Herald*. Available at: http://www.smh.com.au/technology/security/rudd-hackers-escalate-threats-against-govau-websites-20090911-fk2x.html [Accessed May 30, 2010].

Moses, A., 2009d. Qantas censors anti-censorship ad. *The Sydney Morning Herald*. Available at: http://www.smh.com.au/technology/biz-tech/qantas-censors-anticensorship-ad-20090714-djgo.html [Accessed May 31, 2010].

Moses, A., 2008. Net censorship plan backlash. *The Sydney Morning Herald*. Available at: http://www.smh.com.au/news/technology/biztech/net-censorship-plan-backlash/2008/11/11/1226318639085.html [Accessed May 26, 2010].

Moses, A., 2008a. Fatal flaws in website censorship plan, says report. *The Sydney Morning Herald*. Available at: http://www.smh.com.au/news/technology/web/fatal-flaws-in-website-censorship-plan-says-report/2008/12/22/1229794328860.html?page=fullpage [Accessed May 26, 2010].

Mouffe, C., 2005. *On the political*, London & New York: Routledge.

Mouffe, C., 2000. *The democratic paradox*, London: Verso.

Mouffe, C., 2000a. Deliberative democracy or agonistic pluralism. *Reihe Politikwissenschaft / Political Science*, (Series 72). Available at: www.users/unimi.it/dikeius/pw_72.pdf [Accessed May 26, 2010].

Mouffe, C., 1999. Deliberative democracy or agonistic pluralism? *Social Research*, (66: 3), 746-58.

Mouffe, C., 1996. Democracy, power and the 'political'. In S. Benhabib, ed. *Democracy and difference: Contesting the Boundaries of the Political*. Princeton, NJ: Princeton University Press, pp. 245-256.

Mouffe, C., 1993. *The return of the political*, London & New York: Verso.

Mouffe, C. & Miessen, M., 2007. Articulated power relations - Markus Miessen in conversation with Chantal Mouffe. Available at: http://roundtable.kein.org/node/545 [Accessed November 21, 2009].

Mungo, P. & Clough, B., 1992. *Approaching zero: The extraordinary underworld of hackers, phreakers, virus writers and keyboard criminals*, New York: Random House.

Murdock, G., 1992. Citizens, consumers and public culture. In K. C. Schroder & M. Skovmand, eds. *Media cultures*. London: Routledge, pp. 17-41.

Murdock, G. & Golding, P., 2005. Culture, communications and political economy. In J. Curran & M. Gurevitch, eds. *Mass media and society*. London & New York: Oxford University Press & Hodder Arnold, pp. 60-83.

Murdock, G. & Golding, P., 2004. Dismantling the digital divide: Rethinking the dynamics of participation and exclusion. In A. Calabrese & C. Sparks, eds. *Toward a political economy of culture: Capitalism and communication in the twenty-first century*. Lanham, Maryland: Rowman & Littlefield Publishers, Inc., pp. 244-260.

Murdock, G. & Golding, P., 1973. For a political economy of mass communication. In R. Milliband, ed. *Socialist register*. London: The Merlin Press Ltd.

Napoli, P.M., 2008. The Internet and the forces of 'massification'. *Electronic Journal of Communication*, (8(2)). Available at: http://www.cios.org/www/ejc/v8n298.htm [Accessed May 26, 2010].

National Classification Code 2005. *Commonwealth of Australian Law*. Available at: http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200508203?OpenDocument [Accessed May 26, 2010].

Negroponte, N., 1998. Beyond digital. *Wired*, (6(12)), 288.

Negroponte, N., 1995. *Being digital*, New York: Knopf Publishing Group.

Negt, O. & Kluge, A., 1993. *Public sphere and experience: Toward an analysis of the bourgeois and proletarian public sphere*, Minneapolis & London: University of Minnesota Press.

New Zealand Internet Blackout. *Wikipedia*. Available at:

http://en.wikipedia.org/wiki/New_Zealand_Internet_Blackout [Accessed May 13, 2010].

Nieminen, H., 2007. Disobedient media - Unruly citizens: Governmental communication in crisis. In B. Cammaerts & N. Carpentier, eds. *Reclaiming the media: Communication rights and democratic media roles*. Bristol & Chicago: Intellect, pp. 176-191.

Nip, J.Y.M., 2004. The relationship Between online and offline communities: The case of the Queer Sisters. *Media, Culture & Society*, 26(3), 409-428.

Nissenbaum, H., 2004. Hackers and the contested ontology of cyberspace. *New Media & Society*, 6(2), 195-217.

Nissenbaum, H. & Introna, L.D., 2004. Shaping the web: Why the politics of search engines matter. In V. V. Gehring, ed. *The Internet in public life*. Maryland: Rowman & Littlefield Publishers Inc., pp. 7-28.

No Clean Feed: Learn. *No Clean Feed*. Available at: http://nocleanfeed.com/learn.html [Accessed May 29, 2010].

Noguiera, A., 2002. The birth and promise of the Indymedia revolution. In B. H. Shephard & R. Hayduk, eds. *From ACT UP to the WTO : Urban protest and community building in the era of globalization*. London: Verso.

Noveck, B.S., 2004. Unchat: Democratic solution for a wired world. In P. M. Shane, ed. *Democracy online: The prospects for political renewal through the Internet*. New York & London: Routledge, pp. 109-121.

Noveck, B., 2000. Paradoxical partners: Electronic communication and electronic democracy. In P. Ferdinand, ed. *The Internet, democracy and democratisation*. London: Routledge, pp. 18-35.

NZ blogs in copyright law blackout demo, 2009. *The Sydney Morning Herald*. Available at: http://news.smh.com.au/breaking-news-world/nz-blogs-in-copyright-law-blackout-demo-20090223-8ez1.html [Accessed May 17, 2010].

NZ political bloggers to blackout websites 23 Feb. in S92A protest. *Creative Freedom Foundation*. Available at: http://creativefreedom.org.nz/story.html?id=146 [Accessed May 14, 2010].

Oates, S. & Gibson, R.K., 2006. The Internet, civil society and democracy: A comparative perspective. In S. Oates, D. Owen, & R. K. Gibson, eds. *The Internet and politics: Citizens, voters and activists*. New York: Routledge, pp. 1-19.

Olson, M., 1993. Dictatorship, democracy and development. *American Political Science Review*, (87 (June)), 567-76.

Onstad, K. & Rose, B.W., 1996. Is this any way to run cyberspace? Why the hacker ethos is bad for the Net. *Canadian Business*, 69(42), 5.

Open Internet. *Open Internet*. Available at: http://openinternet.com.au/learn_more/ [Accessed May 26, 2010].

Operation Didgeridie. *Insurgen.info*. Available at: http://insurgen.info/wiki/Operation_Didgeridie [Accessed May 26, 2010].

Operation Titstorm. *Encyclopedia Dramatica*. Available at: http://encyclopediadramatica.com/Operation_Titstorm [Accessed May 31, 2010].

Operation Titstorm - Why We Protest. *Why We Protest*. Available at: http://forums.whyweprotest.net/292-freedom-expression/operation-titstorm-61002/ [Accessed April 16, 2010].

Örnebring, H., 2007. A necessary profession for the modern age? Nineteenth century news, journalism and the public sphere. In R. Butsch, ed. *Media and public spheres*. Hampshire & New York: Palgrave MacMillan, pp. 71-82.

Our Goals (CFF). *Creative Freedom Foundation*. Available at: http://creativefreedom.org.nz/goals.html [Accessed May 13, 2010].

Ozimek, J., 2010. Aussie net censorship turning Chinese. *The Register*. Available at: http://www.theregister.co.uk/2010/02/14/aussie_firewall_latest/ [Accessed May 30, 2010].

Padovani, C., Tuzzi, A. & Nesti, G., 2007. Communication and (e)democracy: Assessing European e-democracy discourses. In B. Cammaerts & N. Carpentier, eds. *Reclaiming the media: Communication rights and democratic media roles*. Bristol & Chicago: Intellect, pp. 31-65.

Palczewski, C.H., 2001. Cyber-movements, new social movements and counter-publics. In D. Brouwer & R. Asen, eds. *Counterpublics and the state*. New York: SUNY Press, pp. 9-27.

Palmer, G., 2000. The new spectacle of crime. In D. Thomas & B. D. Loader, eds. *Cybercrime: Law enforcement, security and surveillance in the information age*. London and New York: Routledge.

Papacharissi, Z., 2002. The virtual sphere: The Internet as a public sphere. *New Media & Society*, 4(1), 5-23.

Patalong, F., 2009. Protestkultur: Anonymer angriff aus dem Web. *Der Spiegel*. Available at: http://www.spiegel.de/netzwelt/netzpolitik/0,1518,648653,00.html [Accessed May 30, 2010].

Patelis, K., 2000. E-mediation by America Online. In R. Rogers, ed. *Preferred*

placement: Knowledge politics on the web. Masstricht, the Netherlands: Jan van Eyck Akadamie.

Patelis, K., The political economy of the Internet. In J. Curran, ed. *Media organisations in society*. London: Arnold.

Patten, F., 2010. Depictions of female orgasm being banned by classification board. *The Australian Sex Party*. Available at: http://www.sexparty.org.au/index.php/press-releases/619-depictions-of-female-orgasm-being-banned-by-classification-board [Accessed May 30, 2010].

Perkins, N., 2010. Attacks on government websites must be condemned. *Stop Internet Censorship*. Available at: http://www.stopinternetcensorship.org/207-media-release-attacks-on-government-websites-must-be-condemned.html [Accessed August 23, 2010].

Peters, B., 2002. Concepts of public deliberation - Some challenges, some revisions.

Pew Internet and American Life Project. *Pew Internet and American Life Project*. Available at: http://www.pewinternet.org/ [Accessed May 9, 2010].

Phelan, J.M., 1991. Selling consent: The public sphere as a televisual market-place. In P. Dahlgren & C. Sparks, eds. *Communication and citizenship: Journalism and the public sphere in the new media age*. London and New York: Routledge, pp. 75-93.

Pickard, V.W., 2006. United yet autonomous: Indymedia and the struggle to sustain a radical democratic network. *Media, Culture & Society*, 28(3), 315-336.

Pilcher, P., 2009. Guilty by accusation copyright protesters paint it black. *The New Zealand Herald*. Available at: http://www.nzherald.co.nz/technology/news/article.cfm?c_id=5&objectid=10557216 [Accessed May 13, 2010].

Piven, F., 1995. The public sector under siege. In S. Edgell, S. Walklate, & G. Williams, eds. *Debating the future of the public sphere*. Aldershot & Brookfield: Avebury, pp. 9-24.

PM's website hacked, 2009. *The Australian*. Available at: http://www.theaustralian.com.au/news/pms-website-hacked/story-e6frgal6-1225771367093 [Accessed May 30, 2010].

PM's website hacked, 2009. *Sky News*. Available at: http://www.skynews.com.au/topstories/article.aspx?id=371058 [Accessed May 30, 2010].

Political hacktivists turn to web attacks, 2010. *BBC*. Available at: http://news.bbc.co.uk/2/hi/technology/8506698.stm [Accessed August 18,

2010].

Porter, B., 2001. *The Net effect*, Bristol and Portland: Intellect.

Poster, M., 2007. Internet piracy as radical democracy? In L. Dahlberg & E. Siapera, eds. *Radical democracy and the Internet*. Hampshire & New York: Palgrave MacMillan, pp. 207-225.

Poster, M., 2001. *What's the matter with the Internet?*, Minneapolis & London: University of Minnesota Press.

Poster, M., 1997. Cyberdemocracy: The Internet and the public sphere. In D. Holmes, ed. *Virtual politics: Identity and community in cyberspace*. Thousand Oaks, London & New Delhi: Sage Publications, pp. 212-228.

Postmes, T. & Brunsting, S., 2002. Collective action in the age of the Internet: Mass communication and online mobilization. *Social Science Computer Review*, 20(3), 290-301.

Preoteasa, I., 2002. Intellectuals and the public sphere in post-communist Romania: a discourse analytical perspective. *Discourse and Society*, 13(2), 269-292.

'Press Conference with Kofi Annan' (2002). United Nations: Press conference with Kofi Annan and Foreign Minister Kamal Kharrazi
Teheran, Islamic Republic of Iran, 26 January 2002. Available at: http://www.un.org/News/dh/latest/afghan/sg-teheran26.htm [accessed June 1, 2011].

Press Release: Back Orifice. *Back Orifice 2K*. Available at: http://www.bo2k.com/docs/bo2k_pressrelease.html [Accessed May 7, 2010].

Primoratz, I. (2005). State Terrorism. In Primoratz, I. (ed), *Terrorism*, Hampshire & New York, Palgrave MacMillan.

Pro-porn protesters target government websites, 2010. *ABC News*. Available at: zotero://attachment/1295/ [Accessed August 16, 2010].

Project Chanology. *Encyclopedia Dramatica*. Available at: http://encyclopediadramatica.com/PROJECT_CHANOLOGY [Accessed May 29, 2010].

Project Freeweb. *Encyclopedia Dramatica*. Available at: http://encyclopediadramatica.com/Project_Freeweb#Footage_of_the_Great_Uprising [Accessed May 30, 2010].

Protesters say copyright law stripping rights, 2009. *ONE News*. Available at: http://tvnz.co.nz/politics-news/protesters-say-copyright-law-stripping-rights-2496050/video [Accessed May 18, 2010].

Purcell, K. et al., Understanding the participatory news consumer. *Pew Internet and American Life Project*. Available at: http://www.pewinternet.org/Reports/2010/Online-News.aspx [Accessed May 6, 2010].

Pusey, M. & Hamilton, P., 1987. *Jürgen Habermas*, Chichester & New York: Ellis Horwood Ltd. & Tavistock Publications Limited.

Putnam, R., 2000. *Bowling alone: The collapse and revivial of American community*, New York: Simon and Schuster.

Quittner, J. & Slatella, M., 1995. *Masters of deception: The gang that ruled cyberspace*, London: Vintage.

Rabinovitch, E., 2001. Gender and the public sphere: Alternative forms of integration in nineteenth century America. *Sociological Theory*, (19(3)), 344-369.

Ramadge, A., 2008. Second round of Anonymous v Scientology. *News.com.au*. Available at: http://www.news.com.au/technology/second-round-of-anonymous-v-scientology/story-e6frfro0-1111115818537 [Accessed May 25, 2010].

Ramli, D., 2009. Statistics experts label ISP filtering trials unscientific. *ARN*. Available at: http://www.arnnet.com.au/article/312845/statistics_experts_label_isp_filtering_trials_unscientific/ [Accessed May 26, 2010].

Rathmell, A., 2000. Information warfare and sub-state actors: An organizational approach. In D. Thomas & B. D. Loader, eds. *Cybercrime: Law enforcement, security and surveillance in the information age*. London and New York: Routledge.

Raymond, E.S., 1999. *The cathedral and the bazaar: Musings on Linux and open source by an accidental revolutionary*, Cambridge, MA: O'Reilly.

Raymond, E.S., 1993. *The new hacker's dictionary*, Cambridge, MA: MIT Press.

Reisigl, M. & Wodak, R., 2009. The discourse-historical approach. In R. Wodak & M. Meyer, eds. *Methods of critical discourse analysis*. London & Thousand Oaks, CA: Sage, pp. 87-121.

Reitinger, P.R., 2000. Encryption, anonymity and markets: Law enforcement and technology in a free virtual world. In D. Thomas & B. D. Loader, eds. *Cybercrime: Law enforcement, security and surveillance in the information age*. London and New York: Routledge.

Reporters Sans Frontières: Australia. *Reporters Sans Frontières*. Available at: http://en.rsf.org/surveillance-australia,36674.html [Accessed May 26, 2010].

Reporters Sans Frontières: Internet. *Reporters Sans Frontières*. Available at: http://en.rsf.org/internet,225,225.html [Accessed May 9, 2010].

Rheingold, H., 1993. *The virtual community: Homesteading on the electronic frontier*, New York: HarperCollins.

Rhoads, C. & Chao, L., 2009. Iran's Web spying aided by Western technology. *Wall Street Journal*. Available at: http://online.wsj.com/article/SB124562668777335653.html [Accessed May 9, 2010].

Rice, R.E., 2002. Primary issues in Internet use: Access, civic and community involvement and social interaction and expression. In L. A. Lievrouw & S. Livingstone, eds. *Handbook of new media : Social shaping and consequences of ICTs*. London: Sage Publications.

Richardson, D., 1997. Hacker warfare: Threat of the future. *Armada International*, 21(4), 64.

Riley (J.), J., 2010. Internet filter draft legislation delayed. *ITWire*. Available at: http://www.itwire.com/it-policy-news/regulation/37640-internet-filter-draft-legislation-delayed [Accessed May 25, 2010].

Riley, D., 2010. Anonymous targets Australian Gov. over censorship In Operation Titstorm. *The Inquisitr*. Available at: http://www.inquisitr.com/61057/anonymous-targets-australian-gov-over-censorship-in-operation-titstorm/ [Accessed August 18, 2010].

Riley, D., 2010a. 12 hours later, the Anonymous campaign against the Australian Government continues. *The Inquisitr*. Available at: http://www.inquisitr.com/61130/12-hours-later-the-anonymous-campaign-against-the-australian-government-continues/ [Accessed August 18, 2010].

Riley, D., 2010a. Millions of extra sites to be censored as Australian Gov. bans small breasts, female ejaculation. *The Inquisitr*. Available at: http://www.inquisitr.com/59472/millions-of-extra-sites-to-be-censorsed-as-australian-gov-bans-small-breasts-female-ejaculation/ [Accessed May 30, 2010].

Riley, D., 2009. Anonymous vs the Australian Government, play by play live. *The Inquisitr*. Available at: http://www.inquisitr.com/36578/anonymous-vs-the-australian-government-play-by-play-live/ [Accessed May 30, 2010].

Riley, D., 2009a. Anonymous targets Australian Government over Internet Censorship. *The Inquisitr*. Available at: http://www.inquisitr.com/36559/anonymous-targets-australian-government-over-internet-censorship/ [Accessed August 16, 2010].

Roberts, J.M., 2004. John Stuart Mill, free speech and the public sphere: A Bakhtinian critique. In N. Crossley & J. M. Roberts, eds. *After Habermas:*

New perspectives on the public sphere. Oxford: Blackwell Publishing.

Roberts, J.M. & Crossley, N., 2004. Introduction. In N. Crossley & J. M. Roberts, eds. *After Habermas: New perspectives on the public sphere*. Oxford: Blackwell Publishing.

Roche, M., 1995. Recent European and American conceptions of democracy and politics and the public sphere. In S. Edgell, S. Walklate, & G. Williams, eds. *Debating the future of the public sphere*. Aldershot & Brookfield: Avebury, pp. 41--62.

Roscoe, T., 1999. The construction of the World Wide Web audience. *Media, Culture & Society*, 21(5), 673-684.

Rosenkrands, J., 2004. Politicizing Homo economicus: Analysis of anti-corporate websites. In W. van de Donk et al., eds. *Cyberprotest: New media, citizens and social movements*. London and New York: Routledge.

Ross, A., 2000. Hacking away at the counterculture. In J. Thornton, ed. *Theories of the new media*. London: The Athlone Press.

Rossiter, N., 2006. *Organized networks: Media theory, creative labour, new institutions*, Rotterdam: NAi Publishers.

Rowen, H.S., 1995. The tide underneath the 'Third Wave'. *Journal of Democracy*, (6 (Winter)), 52-64.

RTMark: Your Real Corporation Clearinghouse. *RTMark*. Available at: http://www.rtmark.com/ [Accessed May 28, 2010].

Rudd website attacked in filter protest, 2009. *ABC News*. Available at: http://www.abc.net.au/news/stories/2009/09/10/2681642.htm [Accessed May 30, 2010].

Ruffin, O., 2009a. Gary McKinnon should not be extradited to US. *Techradar*. Available at: http://www.techradar.com/news/world-of-tech/gary-mckinnon-should-not-be-extradited-to-us-608000 [Accessed May 7, 2010].

Ruffin, O., 2009b. You can't support free speech while siding with those who oppress it. *Techradar*. Available at: http://www.techradar.com/news/world-of-tech/you-can-t-support-free-speech-while-siding-with-those-who-oppress-it-614124 [Accessed May 7, 2010].

Ruffin, O., 2007. Google, China, and genocide. *Cult of the Dead Cow*. Available at: http://www.cultdeadcow.com/cDc_files/cDc-0409.html [Accessed May 7, 2010].

Ruffin, O., 2002a. Peekabooty update. *Cult of the Dead Cow*. Available at: http://w3.cultdeadcow.com/cms/2002/02/peekabooty-upda.html [Accessed May 7, 2010].

Ruffin, O., 2002b. Waging peace on the Internet. *The Register*. Available at: http://www.theregister.co.uk/2002/04/19/waging_peace_on_the_internet/ [Accessed May 7, 2010].

Ryan, M.P., 1992. Gender and public access: Women's politics in nineteenth century America. In C. Calhoun, ed. *Habermas and the public sphere*. Cambridge, MA & London, England: The MIT Press, pp. 259-287.

Saarinen, J., 2009. Join New Zealand Internet blackout protest against insane copyright law. *The Techsploder*. Available at: http://www.geekzone.co.nz/juha/6247 [Accessed May 13, 2010].

Saarinen, J., 2009b. New copyright act to hit NZ ISPs. *ZDNet*. Available at: http://www.zdnet.com.au/new-copyright-act-to-hit-nz-isps-339294778.htm [Accessed May 13, 2010].

Salazar, J.F., 2003. Articulating an activist imaginary: Internet as counter public sphere in the Mapuche movement. *Media International Australia incorporating Culture and Policy*, 107, 19-30.

Salter, L., 2003. Democracy, new social movements and the Internet: A Habermasian analysis. In M. McCaughey & M. D. Ayers, eds. *Cyberactivism: Online activism in theory and practice*. London & New York: Routledge, pp. 117-144.

Samuel, A.W., 2004. *Hacktivism and the future of political participation*. a thesis submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the subject of Political Science, Harvard University, Cambridge, Massachusetts, Department of Government.

Samuel, A.W., 2003. Hacktivism and the future of democratic discourse. In P. M. Shane, ed. *Democracy online: The prospects for political renewal through the Internet*. New York and London: Routledge.

Sarno, D., 2008. Rise and fall of the Googled swastika. *The Los Angeles Times*. Available at: http://articles.latimes.com/2008/jul/12/entertainment/et-swastika12/2 [Accessed May 24, 2010].

Sassi, S., 2000. The controversies of the Internet and the revitalisation of local political life. In K. L. Hacker & J. van Dijk, eds. *Digital democracy: Issues of theory and practice*. London, Thousand Oaks & New Delhi: Sage Publications, pp. 90-104.

Savigny, H., 2002. Public opinion, political communication and the Internet. *Politics*, 22(1), 1-8.

Sawhney, J. & Lee, S., 2005. Arenas of innovation: Understanding new configurational potentialities of communication technologies. *Media, Culture & Society*, 27(3), 391-414.

Scammell, M., 2003. Citizen consumers: Toward a new marketing of politics? In J. Corner & D. Pels, eds. *Media and the restyling of politics*. London, Thousand Oaks & New Delhi: Sage Publications, pp. 117-136.

ScatterChat press release, 2006. *Cult of the Dead Cow*. Available at: http://w3.cultdeadcow.com/cms/2006/07/scatterchat-pre.html [Accessed May 7, 2010].

ScatterChat: anonymous, secure chat, 2006. *BoingBoing*. Available at: http://www.boingboing.net/2006/07/22/scatterchat_anonymou.html [Accessed May 7, 2010].

Schachtman, N., 2009. Iran activists get assist from 'Anonymous,' Pirate Bay. *Wired*. Available at: http://www.wired.com/dangerroom/2009/06/iran-activists-get-assist-from-anonymous-pirate-bay/ [Accessed May 25, 2010].

Schell, B.H. & Martin, C., 2004. *Cybercrime: A reference handbook*, Santa Barbara, Denver and Oxford: ABC Clio.

Schifferes, S., 2006. Has the Dotcom boom returned? Available at: http://news.bbc.co.uk/go/pr/fr/-/2/hi/business/6036337.stm.

Schiller, H., 2000. *Living in the number one country*, New York: Seven Stories Press.

Schiller, H.I., 2000a. Digitised capitalism: What has changed? In H. Tumbler, ed. *Media power, professionals and policies*. New York: Routledge, pp. 116-126.

Schiller, D., 1999. *Digital capitalism: Networking the global market system*, Cambridge, Mass.: MIT Press.

Schiller, H., 1996. Information deprivation in an information rich society. In G. Gerbner, H. Mowlana, & H. I. Schiller, eds. *Invisible crises: What conglomerate control of media means for America and the world*. Colorado: Westview Press.

Schiller, J.Z., 2007. On becoming the media: Low power FM and the alternative public sphere. In R. Butsch, ed. *Media and public spheres*. Hampshire & New York: Palgrave MacMillan, pp. 122-135.

Schirato, T. & Webb, J., 2003. The public sphere and the media. In T. Schirato & J. Webb, eds. *Understanding globalisation*. London, Thousand Oaks & New Delhi: Sage Publications, pp. 161-186.

Schudson, M., 2003. Click here for democracy: A history and critique of an information-based model of citizenship. In H. Jenkins, D. Thorburn, & B. Seawell, eds. *Democracy and new media*. Cambridge: MIT Press, pp. 49-59.

Schudson, M., 1992. Was there ever a public sphere? If so, when? Reflections of the American case. In C. Calhoun, ed. *Habermas and the public sphere*. Cambridge & London: The MIT Press, pp. 143-163.

Schuler, D., 2003. Reports of the close relationship between democracy and the Internet may have been exaggerated. In H. Jenkins, D. Thorburn, & B. Seawell, eds. *Democracy and new media*. Cambridge: MIT Press, pp. 69-83.

Schuler, D. & Day, P., 2004. Shaping the network society: Opportunities and challenges. In D. Schuler & P. Day, eds. *Shaping the network society: The new role of civil society in cyberspace*. Cambridge: MIT Press, pp. 1-16.

Schultz, T., 2000. Mass media and the concept of interactivity: An exploratory study of online forums and reader email. *Media, Culture and Society*, (22(2)), 205-221.

Sclove, R.E., 2004. Cybersobriety: How a commercially driven Internet threatens the foundations of democratic self-governance and what to do about it. In P. Day & D. Schuler, eds. *Community practice in the network society: Local action/Global interaction*. London & New York: Routledge, pp. 36-51.

Searle, J., 1995. *The construction of social reality*, New York: Free Press.

Section 92 2008 (CFF). *Creative Freedom Foundation*. Available at: http://creativefreedom.org.nz/s92-2008.html [Accessed May 13, 2010].

Section 92A has been delayed!, 2009. *Creative Freedom Foundation*. Available at: http://creativefreedom.org.nz/story.html?id=170 [Accessed May 21, 2010].

Securus Global. *Securus Global*. Available at: http://securusglobal.com/index.html [Accessed May 9, 2010].

Selnow, G.W., 1998. *Electronic whistle stops*, Westport, CT: Praeger.

Selwyn, N., 2004. Reconsidering political and popular understandings of the digital divide. *New Media & Society*, 6(3), 341-362.

Shapiro, A., 1999. *The control revolution: How the Internet is putting individuals in charge and changing the world as we know it*, New York: Public Affairs.

Shapiro, I., 2004. Power and democracy. In F. Engelstad & Ø. Østerud, eds. *Power and democracy: Critical interventions*. Aldershot & Burlington: Ashgate, pp. 11-32.

Sharp, A., 2010. Net nannies take on the freedom fighters. *The Sydney Morning Herald*. Available at: http://www.smh.com.au/technology/technology-news/net-nannies-take-on-the-freedom-fighters-20100416-skfx.html [Accessed May 26, 2010].

Shenk, D., 1997. *Data smog: Surviving the information glut*, New York: Harper Collins.

Shields, P., 2006. Electronic networks, enhanced state surveillance and the ironies of control. *Journal of Creative Communications*, 1(1), 19-38.

Singel, R., 2008. Palin hacker group's all-time greatest hits. *Wired*. Available at: http://www.wired.com/threatlevel/2008/09/palin-hacker-gr/ [Accessed May 25, 2010].

Skogseth, E.G., 2007. Towards fair participation: Recruitment strategies in demonstration. In B. Cammaerts & N. Carpentier, eds. *Reclaiming the media: Communication rights and democratic media roles*. Bristol & Chicago: Intellect, pp. 107-128.

Slatella, M. & Quittner, J., 1995. *Masters of deception: The gang that ruled cyberspace*, New York: HarperCollins.

Slevin, J., 2000. *The Internet and society*, Cambridge and Massachusetts: Polity Press/Blackwell.

Smith, A., 2010. Government online. *Pew Internet and American Life Project*. Available at: http://www.pewinternet.org/Reports/2010/Government-Online.aspx [Accessed May 6, 2010].

Smith, A., 2009. The Internet's role in campaign 2008. *Pew Internet and American Life Project*. Available at: http://www.pewinternet.org/Reports/2009/6--The-Internets-Role-in-Campaign-2008.aspx [Accessed May 6, 2010].

Smith, A. et al., 2009. The Internet and civic engagement. *Pew Internet and American Life Project*. Available at: http://www.pewinternet.org/Reports/2009/15--The-Internet-and-Civic-Engagement.aspx [Accessed May 6, 2010].

Smith, G., 2001. Upon hearing of the electronic bogeyman. In R. Kick, ed. *You are being lied to: The disinformation guide to media distortion, historical whitewashes and cultural myths*. New York: The Disinformation Company Ltd.

Sohn, G.B., 2005. Copyright reform: The next battle for the media reform movement. In R. W. McChesney, R. Newman, & B. Scott, eds. *The future of media: Resistance and reform in the 21st century*. New York: Seven Stories Press.

SourceForge. *SourceForge*. Available at: http://sourceforge.net/ [Accessed May 9, 2010].

Sparks, C., 2005. Media and the global public sphere: An evaluative approach. In W. D. Jong, M. Shaw, & N. Stammers, eds. *Global activism, global media*. London & Ann Arbor: Pluto Press, pp. 43-49.

Sparks, C., 2004. The impact of the Internet on existing media. In A. Calabrese & C. Sparks, eds. *Toward a political economy of culture: Capitalism and communication in the twenty-first century*. Lanham, Maryland: Rowman & Littlefield Publishers, Inc., pp. 307-326.

Sparks, C., 2001. The Internet and the global public sphere. In L. Bennett & R. Entman, eds. *Mediated politics: Communication in the future of democracy*. Cambridge: Cambridge University Press, pp. 75-95.

Squires, J., 1998. In different voices: Deliberative democracy and aesthetic politics. In J. Good & I. Velody, eds. *The politics of postmodernity*. Cambridge, UK: Cambridge University Press.

Stanton, J.J., 2002. Terror in cyberspace: Terrorists will exploit and widen the gap between governing structures and the public. *American Behavioural Scientist*, 45(6), 1017-1032.

Stein, L., 2009. Social movement web use in theory and practice: a content analysis of US movement websites. *New Media and Society*, 11(5), 749-771.

Steiner, L., 1994. Information and culture as commodity. *Critical Studies in Mass Communication*, 11, 92-115.

Sterling, B., 1992. *The hacker crackdown: Law and disorder on the electronic frontier*, New York: Bantam Press.

Sterling, C.H., 2000. US communications industry ownership and the 1996 Telecommunications Act: Watershed or unintended consequences? In H. Tumbler, ed. *Media power, professionals and policies*. New York: Routledge, pp. 56-69.

Still, B., 2007. Hacking for a cause. Available at: http://www.firstmonday.org/issues/issue7_9/still/index.html [Accessed May 26, 2010].

Stolze, T., 2000. A displaced transition: Habermas on the public sphere. In M. Hill & W. Montag, eds. *Masses, classes and the public sphere*. London & New York: Verso, pp. 146-157.

Stromer-Galley, J., 2003. Diversity of political communication on the Internet: User's perspectives. *Journal of Computer-Mediated Communication*, 8(3).

Submission on Section 92A (CFF). *Creative Freedom Foundation*. Available at: http://creativefreedom.org.nz/story.html?id=381 [Accessed May 13, 2010].

Sunstein, C., 2003. The law of group polarization. In J. Fishkin & P. Laslett, eds. *Debating deliberative democracy*. Oxford: Blackwell, pp. 80-101.

Sunstein, C., 2001. *Republic.com*, Princeton, NJ: Princeton University Press.

Tanner, E., 2001. Chilean conversations: Internet forum participants debate Augusto Pinochet's detention. *Journal of Communication*, 51(2), 383-403.

Targ, H., 2006. *Challenging late capitalism, neo-liberal globalisation and militarism: Building a progressive majority*, Chicago: ChangeMaker Publications.

Tarrow, S., 1998. *Power in movement - Social movements and contentious politics*, Cambridge: Cambridge University Press.

Taylor, P.A., 2004. Hacktivism: Resistance is fertile? In C. Summer, ed. *The Blackwell companion to criminology*. Massachusetts: Blackwell Publishing.

Taylor, P.A., 2001. Hacktivism: In search of lost ethics? In D. Wall, ed. *Crime and the Internet*. London and New York: Routledge.

Taylor, P.A., 2000. Hackers: Cyberpunks or Microserfs? In D. Thomas & B. D. Loader, eds. *Cybercrime: Law enforcement, security and surveillance in the information age*. London and New York: Routledge.

Taylor, P.A., 1999. *Hackers: Crime in the digital sublime*, London and New York: Routledge.

The Free Software Definition. *GNU Project - Free Software Foundation*. Available at: http://www.gnu.org/philosophy/free-sw.html [Accessed April 16, 2010].

The Great Australian Internet Blackout. *The Great Australian Internet Blackout*. Available at: http://www.internetblackout.com.au/ [Accessed May 26, 2010].

The Hacktivismo Declaration. *Hacktivismo*. Available at: http://www.hacktivismo.com/public/declarations/en.php [Accessed May 7, 2010].

The HESSLA's Problems. *GNU Project - Free Software Foundation*. Available at: http://www.gnu.org/licenses/hessla.html [Accessed May 7, 2010].

The Universal Declaration of Human Rights. *United Nations*. Available at: http://www.un.org/en/documents/udhr/ [Accessed May 9, 2010].

The Yes Men. *The Yes Men*. Available at: http://theyesmen.org/ [Accessed May 9, 2010].

Thomas, D., 2000. *Hacker culture*, Minneapolis, MN: University of Minnesota Press.

Thomas, D., 2000a. Criminality on the Electronic Frontier: Corporality and the Judicial Construction of the Hacker. In D. Thomas & B. D. Loader, eds. *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. London and New York: Routledge.

Thomas, D. & Loader, B.D., 2000. Introduction: Cybercrime, law enforcement, security and surveillance in the information age. In D. Thomas & B. D. Loader, eds. *Cybercrime: Law enforcement, security and surveillance in the information age*. London and New York: Routledge.

Thompson, B., 2009. The digital age of rights. *BBC*. Available at: http://news.bbc.co.uk/2/hi/technology/8068463.stm [Accessed May 6, 2010].

Thompson, J.B., 1993. The theory of the public sphere. In O. Boyd-Barrett & C. Newbold, eds. *Approaches to media: A reader (1995)*. London, New York, Sydney & Auckland: Arnold, pp. 252-259.

Thompson, J.B., 1988. Mass communication and modern culture: Contribution to a critical theory of ideology. In O. Boyd-Barrett & C. Newbold, eds. *Approaches to media: A reader (1995)*. London, New York, Sydney & Auckland: Arnold, pp. 54-65.

Thompson, M., 2004. Technology and democracy: A cultural theory approach. In F. Engelstad & Ø. Østerud, eds. *Power and democracy: Critical interventions*. Aldershot & Burlington: Ashgate, pp. 185-208.

Tilly, C., 2004. Regimes and contention. In F. Engelstad & Ø. Østerud, eds. *Power and democracy: Critical interventions*. Aldershot & Burlington: Ashgate, pp. 33-56.

Tilly, C. & Tarrow, S., 2006. *Contentious politics*, Boulder & London: Paradigm Publishers.

Toffler, A. & Toffler, H., 1994. *Creating a new civilisation: The politics of the Third Wave*, Atlanta: Turner Publishing.

Tomlin, R.S. et al., 1997. Discourse semantics. In T. A. van Dijk, ed. *Discourse as social interaction (Discourse studies: A multidisciplinary introduction)*. London, Thousand Oaks & New Delhi: Sage, pp. 63-111.

Top Sites in Australia. *Alexa*. Available at: http://www.alexa.com/topsites/countries;1/AU [Accessed May 30, 2010].

Tor: Anonymity online. *Tor Project*. Available at: http://www.torproject.org/ [Accessed May 7, 2010].

Torkington, N., 2009. New Zealand goes black. *O'Reilly Radar*. Available at: http://radar.oreilly.com/2009/02/new-zealand-goes-black.html [Accessed May 13, 2010].

Torkington, N., 2008. The Internet is an opportunity for artists, not a threat. *Creative Freedom Foundation*. Available at: http://creativefreedom.org.nz/opportunity.html [Accessed May 14, 2010].

Transborder Immigrant Tool. *B.A.N.G. Lab*. Available at: http://bang.calit2.net/xborder/ [Accessed May 9, 2010].

Tsagarousianou, R., 1998. Electronic democracy and the public sphere: Opportunities and challenges. In R. Tsagarousianou, D. Tambini, & C. Bryan, eds. *Cyberdemocracy: Technology, citizens and civic networking*. London & New York: Routledge, pp. 167-178.

TUMEKE! NZ blogosphere : Comprehensive New Zealand blogosphere list rankings for political/news blogs based on traffic, links and posts. *Tumeke*. Available at: http://www.nzblogosphere.blogspot.com/ [Accessed May 15, 2010].

Tung, L., 2009. Australian police probe government cyberattack. *ZDNet*. Available at: http://www.zdnet.co.uk/news/security-management/2009/09/09/australian-police-probe-government-cyberattack-39745160/ [Accessed May 30, 2010].

Tungate, M., 2004. *Media monoliths: How great media brands thrive and survive*, London & Sterling, VA: Kogan Page.

Turkle, S., 1995. *Life on the screen: Identity in the age of the Internet*, New York: Simon & Schuster.

Turkle, S., 1984. *The second self: Computers and the human spirit*, London: Granada.

Turner, F., 2006. *From counterculture to cyberculture*, Chicago and London: University of Chicago Press.

Turner, F., 2005. Where the counterculture met the new economy: The WELL and the origins of virtual community. *Technology and Culture*, 46, 485-511.

USGAO, 2010. *Intellectual property: Observations of efforts to quantify the effects of counterfeit ad pirated goods*, U.S. Government Accountability Office. Available at: http://www.gao.gov/products/GAO-10-423.

Vaidhyanathan, S., 2004. *The anarchist in the library: How the clash between freedom and control is hacking the real world and crashing the system*, New York: Basic Books.

Vallance, C., 2010. Activists turn 'hacktivists' on the web. *BBC*. Available at: http://news.bbc.co.uk/2/hi/technology/8567934.stm [Accessed August 18, 2010].

Van Aelst, P. & Walgrave, S., 2004. New media, new movements? The role of the Internet in shaping the 'anti-globalisation' movement. In W. van de Donk et al., eds. *Cyberprotest: New media, citizens and social movements*. London and New York: Routledge.

Vanhanen, T., 1997. *Prospects of democracy: A study of 172 countries*, New York: Routledge.

Vegh, S., 2007. Case illustration: Cyberprotesting globalisation: A case of online activism. In V. Mayer-Schonberger & D. Lazer, eds. *Governance and information technology: From electronic government to information government*. Cambridge, MA., & London: The MIT Press, pp. 208-212.

Vegh, S., 2005. The Media's portrayal of hacking, hackers and hacktivism before and after September 11. *First Monday*. Available at: http://www.firstmonday.org/issues/issue10_2/vegh/ [Accessed May 26, 2010].

Vegh, S., 2003. *Hacking for democracy: A study of the Internet as a political force and its representation in the mainstream media*. University of Maryland, Department of American Studies.

Vegh, S., 2003a. Classifying forms of online activism: The case of cyberprotests against the World Bank. In M. McCaughey & M. D. Ayers, eds. *Cyberactivism: Online activism in theory and practice*. London & New York: Routledge, pp. 71-96.

Vegh, S., 2002. Hacktivists or cyberterrorists? The changing media discourse on hacking. *First Monday*. Available at: http://www.firstmonday.org/issues/issue7_10/vegh/ [Accessed May 26, 2010].

Voiskounsky, A.E., Babaeva, J.D. & Smyslova, O.V., 2000. Attitudes towards computer hacking in Russia. In D. Thomas & B. D. Loader, eds. *Cybercrime: Law enforcement, security and surveillance in the information age*. London and New York: Routledge.

Walzer, M., 2002. Passion and politics. *Philosophy and social criticism*, (28(2)), 617-633.

Warf, B. & Grimes, J., 1997. Counterhegemonic discourses and the Internet. *Geographical Review*, 87: 2, 259-274.

Wark, M., 2004. *A hacker manifesto*, Cambridge: Harvard University Press.

Warner, M., 2002. *Publics and counterpublics*, New York: Zone Books.

Warner, M., 1992. The mass public and the mass subject. In C. Calhoun, ed. *Habermas and the public sphere*. Cambridge & London: The MIT Press, pp. 377-401.

Weber, L.M. & Murray, S., 2004. Interactivity, equality, and the prospects for electronic democracy. In P. M. Shane, ed. *Democracy online: The prospects for political renewal through the Internet*. London & New York: Routledge, pp. 95-108.

Website hacked: 7 News, 2009. *YouTube*. Available at: http://www.youtube.com/v/VlxPwkAtJFI [Accessed May 30, 2010].

Webster, F., 2002. *Theories of information society*, London: Routledge.

Weintraub, J., 1997. The theory and politics of the public/private distinction. In J. Weintraub & K. Kumar, eds. *Public and private in thought and practice*. Chicago and London: The University of Chicago Press, pp. 1-42.

Weisenburger, K., 2001. Hacktivists of the world, divide. *Security Watch*. Available at: http://www.securitywatch.com/tre/042301.html [Accessed May 26, 2010].

Wessler, H. & Schultz, T., 2007. Can the mass media deliberate?: Insights from print media and political talk shows. In R. Butsch, ed. *Media and public spheres*. Hampshire & New York: Palgrave MacMillan, pp. 15-27.

West, D.M., 2005. Democratisation and technological change. In D. M. West, ed. *Digital government: Technology and public sector performance*. Princeton & Oxford: Princeton University Press, pp. 165-184.

What Is Copyright? (CFF). *Creative Freedom Foundation*. Available at: http://creativefreedom.org.nz/copyright.html [Accessed May 13, 2010].

White, S.K., 1988. *The recent works of Jürgen Habermas: Reason, justice & morality*, Cambridge & New York: Cambridge University Press.

Why "Free Software" is better than "Open Source". *GNU Project / The Free Software Foundation*. Available at: http://www.gnu.org/philosophy/free-software-for-freedom.html [Accessed April 16, 2010].

Why We Protest. *Anonymous / Why We Protest*. Available at: http://www.whyweprotest.net/en/ [Accessed May 24, 2010].

Wieczorek, A.E., 2008. Proximisation, common ground, and assertion-based patterns for legitimisation in political discourse. *Critical approaches to discourse analysis across disciplines*, 2(1), 31-48.

Wilhelm, A.G., 2000. *Democracy in the Digital Age: Challenges to Political Life in Cyberspace*, London: Routledge.

Williams, C., 2009. Kiwis go all black over copyright enforcement laws. *The Register*. Available at: http://www.theregister.co.uk/2009/02/17/new_zealand_copyright/ [Accessed May 13, 2010].

Winseck, D., 2002. Netscapes of power: Convergence, consolidation and power in the canadian mediascape. *Media, Culture & Society*, 24(6), 795-819.

Winston, D., 2003. Digital democracy and the new age of reason. In H. Jenkins, D.

Thorburn, & B. Seawell, eds. *Democracy and new media*. Cambridge: MIT Press, pp. 133-142.

Winterford, B. & Hill, J., 2008. ISP-level content filtering won't work. *ZDNet*. Available at: http://www.zdnet.com.au/isp-level-content-filtering-won-t-work-339292158.htm [Accessed May 26, 2010].

Witschge, T., 2004. Online deliberation: Possibilities of the Internet for deliberative democracy. In P. M. Shane, ed. *Democracy online: The prospects for political renewal through the Internet*. London & New York: Routledge, pp. 109-121.

Wodak, R., 1999. Critical discourse analysis at the end of the 20th century. *Research on Language and Social Interaction*, 32, 185-193.

Wodak, R. & Meyer, M., 2009. Critical discourse analysis: history, agenda, theory and methodology. In R. Wodak & M. Meyer, eds. *Methods of critical discourse analysis*. London & Thousand Oaks, CA: Sage, pp. 1-33.

Wolfe, A., 1997. Public and private in theory and practice: Some implications of an uncertain boundary. In J. Weintraub & K. Kumar, eds. *Public and private in thought and practice*. Chicago and London: The University of Chicago Press, pp. 182-203.

Wolfsfeld, G., 1984. Collective political action and media strategy. *Journal of Conflict Resolution*, (28), 363-81.

World Trade Organisation. *World Trade Organisation*. Available at: http://gatt.org/ [Accessed May 9, 2010].

Wray, S., 1998. Electronic civil disobedience and the World Wide Web of hacktivism: A mapping of extraparliamentarian direct action net politics. Available at: http://switch.sjsu.edu/web/v4n2/stefan/ [Accessed May 26, 2010].

Wright, S., 2004. Informing, communicating and ICTs in contemporary anti-capitalist movements. In W. van de Donk et al., eds. *Cyberprotest: New media, citizens and social movements*. London and New York: Routledge.

Wu, Y., 2007. Blurring boundaries in a 'cyber-greater China': Are Internet bulletin boards constructing the public sphere in China? In R. Butsch, ed. *Media and public spheres*. Hampshire & New York: Palgrave MacMillan, pp. 210-222.

Wynne, B., 1988. Unruly technology: Practical rules, impractical discourses and public understanding. *Social Studies of Science*, 18(1), 147-167.

XeroBank Browser. *Wikipedia*. Available at: http://en.wikipedia.org/wiki/XeroBank_Browser [Accessed May 7, 2010].

Yar, M., 2005. The global 'epidemic' of movie 'piracy': Crime-wave or social

construction? *Media, Culture & Society*, 27(5), 677-696.

Young, I., 2001. Activist challenges to deliberative democracy. *Political Theory*, 29(5), 670-690.

Young, I.M., 1997. Difference as a resource for democratic communication. In J. Bohman & W. Rehg, eds. *Deliberative democracy*. Cambridge, MA & London: The MIT Press, pp. 383-406.

Young, I., 1996. Communication and the other: Beyond deliberative democracy. In S. Benhabib, ed. *Democracy and difference*. Princeton, NJ: Princeton University Press.

Young, I.M., 1987. Impartiality and the civic public: Some implications of feminist critiques of moral and political theory. In S. Benhabib & D. Cornell, eds. *Feminism as critique: Essays on the politics of gender in late-capitalist societies*. Cambridge, UK: Polity Press.

Zeller Jr., T., 2006. House member criticizes Internet companies for practices in China. *New York Times*. Available at: http://www.nytimes.com/2006/02/15/technology/15cnd-internet.html?_r=1 [Accessed May 9, 2010].

Zetter, K., 2009. 'Anonymous' declares war on Australia over Internet filtering. *Wired*. Available at: http://www.wired.com/threatlevel/2009/09/anonymous-hacks-australia/ [Accessed May 30, 2010].

Zhao, Y., 2003. Falun Gong, identity, and the struggle over meaning inside and outside China. In N. Couldry & J. Curran, eds. *Contesting media power: Alternative media in a networked world*. Lanham: Rowman & Littlefield.

Zorz, Z., 2010. Government sites crumple under Operation Titstorm's DDoS attack. *Help Net Security*. Available at: http://www.net-security.org/secworld.php?id=8856 [Accessed August 14, 2010].