Handmaiden at Work: Sina Weibo and Internet Censorship in China

by

Lianrui Jia

A thesis submitted to the Faculty of Graduate and Postdoctoral Affairs in partial fulfillment of the requirements for the degree of

Master of Arts

in

Communication Studies

Carleton University
Ottawa, Ontario

Abstract

With the world's biggest internet population and the most complicated internet control system, the internet in China has incited great hopes and fears about the impacts this new medium of communication might have on society. In this thesis, I contend that neither the dystopic view nor the utopic view of how internet challenges the authoritarian rule in China helps us to understand the elaborate system of Chinese internet regulation and control. Instead, I argue, we need to contextualize the development of the Chinese internet against the backdrop of the country's larger political economy and in relation to how internet controls have been enabled through the legal and regulatory environment and the participation and coordination of state actors, private internet companies and end users. The role of private internet companies is emphasized through the case study of Sina Weibo. Sina Weibo, I argue, exemplifies how such processes are being delegated by the state to private internet companies in China writ large, thereby carving out a new type of regime of internet control and regulation, while also distinguishing the Chinese internet from the larger global internet of which it is a part.

Acknowledgement

This thesis would not have been possible without the support and help of the following people.

First and foremost, my deepest gratitude goes to my thesis supervisor, Professor Dwayne Winseck. Professor Winseck's has provided a strong pillar of support both in guiding this thesis and throughout my entire M.A studies. Dr. Tokunbo Ojo and Dr. Sandra Robinson have also offered generous help, encouragement and guidance throughout my undergraduate and graduate degrees in Carleton University. They are my role models. I also wish to thank Professor Sheryl Hamilton, Professor Ira Wagman, Professor Eileen Saunders, and Coleen Kornelson for their help and encouragement in every step of the way.

I am also deeply grateful for having a loving and supporting cohort: Emily, Jill, Lauren, Masoud, Justine, Gabrielle and Nirvmal. Their company makes our journey together so much more pleasant and memorable.

To friends from near or afar: Xiaofang, Xiaofei, and Yiyang. I owe a deep debt of gratitude to your support and encouragement during the writing of this thesis. Especially, I wish to thank Ato for his help in the editing of this thesis and in challenging me to think outside the box.

Last but not least, this thesis would not have been possible without my friend, my teacher, and my mother, Yurong. She supports me in all her capacity and loves me unconditionally through good times and bad. My youthful sisters, Yi and Jia, also showed love and concerns in their own, unique ways during the writing of this thesis. I am truly grateful for having them in my life.

Table of Contents

List of Tables

List of Figures

1 Chapter: Introduction

> … because technological innovation is inextricably linked to processes of social reconstruction, any society that hopes to control its own structural evolution must confront each significant set of technological possibilities with scrupulous care.
> — Langdon Winner, *The Whale and The Reactor*

The internet constitutes part of the socio-technical structure that underpins our society. It is closely interwoven with our everyday existence and colours our perceptions, thoughts and behavior. As a human construction, it reflects the choices that have been made regarding technology and the values of a society that has made such choices. With the world's biggest internet population and the most sophisticated internet control system, the internet in China has incited great hopes and fears about politics and technology. I contend that given the humanly constructed nature of the internet, neither the dystopic view nor the utopic view of how the internet affects authoritarian rule in China offer a sound view of the current processes of internet regulation and control in China. Instead, we should contextualize the development of the Chinese internet against the backdrop of the country's larger political economy, with a clear focus on how internet control is enabled through the participation and coordination of state actors, private internet companies and end users, while ultimately being embodied in a specific legal and regulatory setting. This thesis examines how private internet companies in China, adapt to and assume the state's requirements that they actively police online content and integrate political controls into the commercial internet services they deliver to end users. This thesis examines how these and other measures of cyberspace control have been formalized and institutionalized in China, specifically within the legal and regulatory framework that undergirds the internet in China.

1.1 Thesis Statement and Research Questions

This thesis seeks to answer these following questions:

- Who are the main stakeholders in the Chinese internet control system?
- What role does private enterprise play in the internet control processes?
- How do internet enterprises integrate overt and covert information into the services they deliver and the business models upon which they are based?

These are important questions that not only address the technologies of control at the heart of the Chinese internet – the content, speed and myriad techniques of the state's control mechanism – but also how this power to shape the social flow of information is structured through a dynamic process of interaction between the state, private internet companies and the public.

To map out the legal and regulatory framework of Chinese internet control, I will employ Thomas Misa's (1999) multi-scalar, three-layered method of studying socio-technical infrastructure. At the *macro-level*, I will situate the discussion about Chinese internet control against the backdrop of the country's historical legacy of media control and argue that the development and expansion of the internet exhibits both continuities and breaks in relation to the control systems that have long been applied to the telecommunication industry and mass media. At the *meso-level*, I will provide an overview of the regulators and regulations of private internet companies in China. And finally, at the *micro-level*, I will examine how one private internet company, Sina Corp., assumes and formalizes political control through its user contracts, terms of service and the design of the microblogging service it provides to users.

I choose Sina Corp. as the object of the central case study in this thesis for two key reasons. First, because Weibo, the Twitter-like microblogging services offered by Sina Corp.,

is the largest of its kind amongst Chinese users and is said to be one of the most active social media platforms in China with 600 million registered users. Weibo *enables* many forms of interaction – social, commercial, personal, political – but it also *constrains* how people communicate and interact with one another by filtering, blocking and censoring what its users can say and see. Given the impact and dominance of Weibo among Chinese internet users, its influence is widely recognized by government officials. For example, as of March 2011, more than 1,708 government officials and 720 organizations have launched their own microblog accounts and utilized Weibo as means to communicate and interact with the public (Zhang and Jia, 2011).

Secondly, not only has Weibo quickly gained a leading position in the domestic market, it has also actively expanded into the international market by launching its Initial Public Offering on NASDAQ in April 2014. In fact, Weibo has achieved extraordinary success as a business *despite* the political controls that have been imposed on the company and the internet by the Chinese government. Weibo exemplifies how internet companies operate, survive, and even thrive, in an authoritarian country. Weibo's business model, its close relationship with the Chinese government, and the accessibility of the company's information make it a good focus for research into the subject at hand. Indeed, as a publicly-listed company on the New York Stock Exchange, there is a relatively high level of detailed information about the company available in its financial reporting documents. These documents, in turn, offer much insight into how the company survives and even thrives within the tightly controlled Chinese media system and how it has grown despite, or perhaps even because of, the thicket of regulations that encompass the internet in China[1].

[1] Such as the Real Name Registration Policy established in 2011 and the government's campaign that targets online rumors in 2012 and 2013.

1.2 Key terms and Significance

Given the interdisciplinary nature of internet studies, varying from Science and Technology Studies (STS), political science and communication studies, it is important to be explicit about the meaning of the key terms and concepts I will use in this thesis.

Firstly, as Langdon Winner (1986) states, "technology has expanded rapidly in both its denotative and connotative meanings" and "the word has become to mean everything and anything" (pp. 8-11). The social meaning of technology is unstable and changes over time: for example, in the early twentieth century, it referred to required skills, machines and systems and by the middle of the twentieth century, it implied the systems of machines and techniques (Nye, 2006, p. 15). As a form of technology, the internet has different meanings to different people in various stages of its development. However, in this thesis, I refer to the internet not only as a form of technology, but also as an infrastructure, a large sociotechnical system. As an infrastructure, the internet is not invisible, or "natural": it does not reside quietly in the background or as part of nature but needs maintenance; it constitutes both physical and intangible elements; it breaks down and has vulnerabilities; it is subject to choices made in society; it is, essentially, a man-made sociotechnical system (Edwards, 2011).

Secondly**,** "internet control" implies a wide range and forms of activities. For example, control not only implies control over physical network infrastructures (e.g. decision over where a nation's international internet gateway is built), but also control over the flow of information (such as licensing, screening and editorial control and installation of censorship software in cyber cafés), and technical control processes that are often invisible to users, such as automated-computer censorship. Last but not least, there are also more subtle forms of control, such as self-censorship that take place among internet users. Given the wide range of

control activities, it is essential to point to the specific types of control that this thesis focuses on: namely, those forms of control that have been formalized in policies and regulations as well as in the Online Service Provider's *User Contract*, or "terms of service" agreements. The conditions in *Term of Service* agreements, and in laws regulating internet companies in China, are important because they set out the condition under which business operates in the Chinese market. At the same time, focusing on the control processes that are formalized in regulations does not mean that other forms of control on the Chinese internet can be ignored. In fact, the existing literature from computer science and engineering often unveils the opaque technical means used to block the free flow of information. Such research helps us to understand how a complex and wide-ranging system of internet controls has been built up with respect to the Chinese internet.

When talking about internet control in China, I will use the term "control mechanism", "system of control" or "control processes" to refer to the cooperative nature of cyberspace controls. Many mainstream news reports often refer to the Chinese internet control system as the "Great Firewall of China" (e.g. The Economist, 2013; Dai, 2000). I agree with Lokman Tsui's argument, however, that such terms should be used with extra caution. As Tsui (2007) argues, the "Great Firewall of China" (GFW) is a problematic metaphor and a myth that often implies the Chinese government only censors information coming from outside, as if the Great Firewall was initially built to keep the "barbarians" out of the country. Séverine Arsène (2012) further suggests that the Great Firewall metaphor fails to capture the range of actors that are exerting control over the internet in China, most significantly, the private internet companies (p.3).

Thirdly, the Great Firewall metaphor is also limited in capturing the agency of Chinese internet users. Although this study focuses on various means of controls imposed by the state and delegated to private sector actors, this does not mean that citizens are powerless in resisting or exerting cyberspace control. In fact, internet users' means of resistance is as diverse as the existing means of control. Inspired by such a rigidly controlled system, Chinese internet users' resistance and circumvention tactics come in various forms: cultural, social and technical. This thesis identifies and elaborates on some of these forms of control. The creative resistance to and circumvention of information controls in China is nothing new given the strict legacy of media control in China. Prior to the advent of the internet in China, illegal satellite dishes, for instance, were installed in China to receive information from blocked sources in the West. Thus, it is not so surprising that as the internet grows more popular, Chinese citizen's resistance has adapted to the new technological conditions. Initially, instead of directly sending an email to one another, for example, many expatriate Chinese sent a PDF of their email message to avoid censorship. More recently, web users have shown their discontent with the government's clampdown on information flows on the internet through linguistic means such as the clever use of metaphors (see, for example, China Digital Times' *Grass Mud Horse Lexicon*). At the same time, various circumvention software and proxy servers are also being employed by tech-savvy users to "climb over the Great Firewall" (Robinson & Yu, 2013).

Internet users in China are not a homogenous group. In fact, ordinary internet users can also exert control over online discussions on behalf of the Chinese government. This is exemplified by the "50 cent Party", a group of college students paid by the Party to post pro-Party comments (i.e. 50 cents RMB for each post).

The significance of this project is three-pronged. Firstly, by exploring the key players and the legal framework that underpins the Chinese internet control processes, I want to gain a fuller understanding of the increasingly privatized system of internet controls in China. In particular, I hope this study will help to illustrate that internet censorship is not a straight-forward process but in fact, and diverging from the common perception that Chinese internet users are repressed, angry, or "live in the dark", the current generation of internet controls have gained a certain level of legitimacy among the public. This public legitimacy is consistently demonstrated through a series of surveys conducted, for example, by the Chinese Academy of Social Sciences from 2001 to 2007 on *Internet Usage and its Impact in Seven Chinese Cities*.[2] These reports reveal a rather staggering fact: despite criticism of China's internet control system and the rigid information censorship that the Chinese government has implemented over cyberspace, 67.8 percent of surveyed participants (2,063 people in total) agreed that the "Internet should be managed or controlled" (Guo, 2001). The approval ratings even spiked to 86.1 percent in 2003, while the percentage remained stable around 82 percent in year 2004 and 2007 (Guo, 2007). Moreover, when asked what types of information should be managed and controlled, 49 percent of all surveyed internet users agreed that political content was a proper target of regulation (ibid.). Such consent illustrates that not only does the Chinese government manage and control the internet effectively, but also it enjoys a fairly high degree of public legitimacy. Informed by such finding, this project aims to show that, rather than a zero sum game between state and citizens, internet control in China is not only a process composed by the state's technical measures that block and filter access but also the legal, social and cultural norms that are aided and abetted by private businesses.

[2] The survey was discontinued after 2007.

Although studies of the Chinese internet come from multiple disciplines, the pre-dominant scope is still about the relationship between internet and political change. As Bingchun Meng (2010) argues, "the pre-formed lens of democratization [is] becom[ing] so dominant in Chinese Internet studies that it excludes alternate ways of framing new research" (p. 501). She further observes that the emphasis on democratic changes is often based on a narrow understanding of politics, and fails to acknowledge the heterogeneity of internet users and their online activities (Meng, 2010). In fact, as more people gain access to the internet through computers, mobile phones and devices, various social groups will appropriate the internet for different purposes. As the 2013 Chinese Internet and Network Information Center (CNNIC) report shows, two of the fastest growing internet uses in the country are for entertainment (music, video, games and literature) and e-commerce (group-buying, resembling that of Groupon in the West, for example, and which showed a 21.2% increase in user's adoption rate compared to that of 2012) (CNNIC, 2013). In other words, the utopia-dystopia binary of whether the internet will democratize China or bolster its one-party State is too crude a view of the matters at hand. We need a better and richer account of the cross-cutting trends and developments with respect to the Chinese internet and its regulability, governance and control.

Secondly, this study aims to map the legal and regulatory architecture of the Chinese internet control system, which is often an important aspect of the control processes that some of the current quantitative studies fail to capture. Much of the existing literature on Chinese internet studies provide a fairly comprehensive picture of the different mechanisms of internet control and censorship from a computer science perspective (Fu, Chan, & Chau, 2013; Crandall, et al., 2013; King, Pan, & Roberst, 2013; Ng, 2013; Wright, 2013). These studies

tend to focus on the content and methods of internet censorship, such as studying what types of content are censored and how fast content is censored, blocked and removed after it has been posted online. These studies, however informative, are often limited by their temporary focus on specific case events given that the censored content is often subject to the political context of the moment and varies across different geographic regions of what is, after all, a vast and varied country.

On the other hand, there is too little emphasis on how censorship, control and self-discipline is formalized, and institutionalized, in China. By focusing primarily on the people and institutions that "control", these studies often fail to address how control and power is structured at the institutional level and how it is normalized, justified, encouraged and sustained in the day-to-day communication between internet companies and internet users. As Robin Mansell (2003) poignantly puts it, research on new media tends to only provide a "fragmentary picture of how our experience of technological mediation is being produced and reproduced" and such tunnel vision also neglects "political economy analysis… (and) overall social and economic dynamics of the production and the consumption of new media". This thesis aims to address this gap by looking at the interplay between power, politics and economics in the regulation of the internet and how the state carves out a legal and regulatory environment to mobilize private internet companies to censor web content and otherwise regulating their users while embracing the economic potential of the internet.

Thirdly, this study also has real world implications. The rise of Chinese media enterprises not only affects people's right to access information but has also begun to exert considerable influence on communication around the globe. The market dominance of Weibo makes the company a role model for other microblogging service providers. As the country's

leading microblog service, how Sina approaches the state delegated task of monitoring and regulating online discussion and a much wider list of responsibilities, as we will see, serves as a model for other microblogging services, not just in China but in other countries as well. The Beijing Municipal's 2011 *Real Name Registration Policy* targeting Weibo, for instance, requires users to register with their real ID on the backstage while allowing them to use a pseudo name as their Weibo account name. This municipal level legal initiative was later formalized at the national level and then applied to other Chinese microblogging services such as Tencent Weibo and Netease Weibo.

The interconnectedness and interdependencies in the development of the global information infrastructure also means that internet control processes implemented on domestic Chinese internet companies have already had several unintended global implications. Firstly, as internet control grows into a global norm in both authoritarian and democratic countries, the quasi-privatized control system in China has been "exported" to and emulated by other autocratic countries, such as Iran (MacKinnon, 2010, 2012; Mueller, 2012). In addition, some network hardware designed in China for surveillance purposes is being exported to countries in Africa, South American and the Middle East (Jiang, 2010; MacKinnon, 2012). Software and applications developed by Chinese tech companies, such as live chat applications QQ and WeChat, have also gained popularity around the globe. Messages sent using WeChat, although from countries outside China, e.g. from Thailand to Singapore, are subject to censorship in China because the censored words are coded in the application (Millward, 2013; Crandall, et al., 2013). Even the technical arrangement of internet traffic that bypasses China, such as routing arrangement among Online Service Providers (e.g. Facebook and YouTube), have resulted in, for example, several instances of temporary service shutdown for users outside

China (Mueller, 2012). These "spill over" effects of Chinese internet control concern not only users and consumers in China, therefore, but also their counterparts, policy makers and scholars in other countries.

More importantly, the internet is not only a virtual space, but also a lived experience that has real-life consequences. This is especially evident in authoritarian countries where people have been jailed because of an email they have sent; bloggers are banned from expressing themselves out of fear of retribution for posts they have written; and people who work as web censors are under constant pressure to follow the Party guidelines in order to keep their jobs and to make a living. In a highly mediated digital communication environment, therefore, internet intermediaries play a vital role in safeguarding the rights of internet users, and we need to understand the conditions that both constrain and enable their ability to play such a role as carefully and as systematically as we can.

1.3 Thesis Outline

This thesis aims to provide a contextualized and historical discussion of Chinese internet controls with an emphasis on how the development and implementation of these controls is achieved through coordinated activities between the state and private companies. Chapter 1 reviews the existing literature on internet controls, with a focus mainly on three bodies of literature: first, writings about the internet as a complex sociotechnical system that is, despite common-place claims to the contrary, quite controllable; second, the chapter reviews the literature on new forms of governance that are being brought about because of the challenges the internet poses to traditional modes of state intervention and regulation; and lastly, but not least, I will conduct a systematic review on Chinese internet controls and a review of existing literature on Sina Weibo and its implications for Chinese internet controls.

Chapter 2 reviews the theoretical and methodological foundations that underpin the thesis. Of particular importance in this regard are Andrew Feenberg's theorization of the "double aspect" of technology and Langdon Winner's theory of technological politics. Significant attention is also given to the ideas of Lawrence Lessig, Yochai Benkler, Jonathan Zittrain and Craig MacTaggart regarding the 'regulable' internet. A series of studies by the OpenNet Initiative that portray the evolution of three generations of internet control over time is also examined, as are different attempts to theorize the role of the state in relation to internet regulation (MacKinnon, Jiang, Mueller, Goldsmith and Wu). Chapter 2 concludes with a discussion on the research methodology used in this thesis.

In Chapter 3, I situate the discussion of contemporary internet controls against the backdrop of China's historical legacy of media control. I argue that the development of the internet exhibits many continuities with the development of telecommunications in China over a much longer period of time, while also outlining some of the key challenges, hurdles and vulnerabilities associated with the government's attempt to transpose the same control systems that have long been a mainstay for the telecommunication industry to the internet. Government policies, key regulatory texts, legal texts, influential statements issued by the various ministries involved in media regulation, such the government's white paper, *The Internet in China* (IOSC, 2010), are used extensively to sketch the contours of the internet control system that has taken shape in China since the late 1990s.

Chapter 4 sketches the main regulatory conditions under which private internet companies operate in China. It focuses on the system of rules the government has established with respect to internet content regulation, licensing requirements, and the responsibilities of internet intermediaries with respect to content available online and the behaviour of their users.

The chapter also critically examines the rules regarding the ownership and regulation of the telecommunications sector China agreed to when it joined the WTO in 2001. The aim is to critically examine the formalization of government internet controls in China over time and how private companies have been enrolled ever more deeply into the government's elaborate and evolving system of internet controls.

Chapter 5 examines how Sina Weibo – one of China's largest internet companies – has seamlessly integrated internet monitoring, data retention and disclosure practices into its day-to-day activities at the behest of the government and, crucially, how these capabilities are experienced by the company's users. The chapter hones in on how Sina Weibo's *Terms of Service,* User Verification system and User Credit system condition people's experience and use of the service. These banal design elements of the website, as will be seen, are hardly inconsequential. Instead, by examining these mundane and typically taken-for-granted aspects of the internet we get a clear view of how self-censorship is actually being "built into" the very technological foundations of the internet, often without users' awareness or their consent. The concluding chapter recaps the main findings and arguments of the thesis and highlights some of their possible implications for Chinese internet research and researchers.

2 Chapter: Literature Review

Given the sociopolitical significance in studying internet control in China, and the interdisciplinary nature of internet studies, the amount of theoretical work on this topic is vast, spanning disciplines from political science, anthropology, sociology, science and technology studies (STS) as well as communication, media and information studies. To help structure what otherwise is a long and tangled list of relevant research, it is useful to organize the relevant literature into three categories: the first examines the internet as a sociotechnical system and dissects its underlying architecture and composition. This body of research helps us to uncover the social and political dimensions of the internet and raises substantial doubts about those accounts that cast the internet as largely a benign and neutral technology. By demonstrating the complexity of the technical architecture that constitutes the internet, these studies counter common claims about the anarchistic and unregulable nature of the internet. Instead, this literature suggests that the layered architecture of the internet makes it hard but not impossible to regulate.

The second body of literature addresses how the internet has led to the creation of unique forms of governance that challenge the traditional nation state rule and how nation states, especially authoritarian states, have responded to threats to their authority by mobilizing the private sector and various legal and technical means to assert control over the internet. These studies provide many useful conceptualization of how the state's control over the internet has evolved over time and how that influence is exercised through a combination of market, cultural, legal and technological means, in line with views that Lawrence Lessig (1999) set out in his classic text on the topic, *Code and Other Laws of Cyberspace*.

The third body of literature examined hones in on studies of Chinese internet control. These studies come from multiple disciplines and employ different research methodologies but generally offer insight into the nuts and bolts of internet censorship processes in China. I also review the literature that focuses on Sina specifically, and especially the issue of how the company copes with the state's tight political controls while also striving to maximize its profit.

2.1 Internet as a Sociotechnical System

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. We have no elected government…cyberspace does not lie within your borders… We are forming our own Social Contract… our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge. We will create **a** civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.
> - John Perry Barlow A *Declaration of the Independence of Cyberspace, 1996*

The self-styled "Thomas Jefferson" of the Internet, the founding father of the Electronic Frontier Foundation, John Perry Barlow, wrote this passage in 1996 to defend cyberspace from the *Communication Decency Act* (CDA) that aimed to punish all transmission of "indecent" sexual communications or images on the Internet "in a manner available to a person under 18 years of age" (Wu, p. 19). Written in the early days of the internet, this passage captures perfectly how the internet was perceived by cyber-libertarians: it is immaterial, untraceable and unidentifiable; it is a space without boundaries; it is a virtual space separate from real world regulations and laws; it is a self-governing and disciplined body; it is, in sum, an egalitarian utopia for civilization.

Quite contrary to Barlow's vision of how the internet should be, the internet's development path has rarely followed the utopian script that he and others imagined. Crucially, the internet is more than a virtual space that functions separately from the real world. As the following conceptualizations of cyberspace demonstrate, the internet, as a layered structure, is in fact, a composition of both material infrastructures, equipment, devices, as well as many immaterial elements, such as codes, domain names, and software programs. Yochai Benkler, Craig McTaggart, Jonathan Zittiran, and Lawrence Lessig, amongst others, provide a useful and comprehensive anatomy of the complex technical system that we call the internet. While their analyses unfold at different levels of abstraction and for different purposes, they answer two fundamental questions that are centrally relevant to this thesis: what constitutes the internet? Is it regulable?

In *the Wealth of Networks*, Yochai Benkler provides a typology of core resources that are necessary for mediated information production and exchange. He categorizes them into three layers according to the distinctive characteristics of the components that make up each layer: the physical layer, logical layer and content layer (See Table 1). The *physical layer* contains both transmission channels and devices for producing and communicating information (Benkler, 2006, p. 396). At this layer, the common carriage principle is core in order to ensure a neutral, end-to-end and user-centric network. The *logical layer* mainly comprises algorithms and protocols. Open access to such protocols and algorithms is valued to ensure transparency between different links in the chain of internet-mediated communications (ibid). The *content layer* consists of existing knowledge and information, underpinned by the normative value that the "public good"

feature of information should be safeguarded in order to maximize access to knowledge because knowledge is the basis of human development and future innovation.

Table 1

Yochai Benkler's Typology of Key Resources in Information and Knowledge Production

Layer	Content	Golden principle
Physical layer	Transmission channels, devices	Common Carriage
Logical layer	Algorithm and protocols	Open access
Content layer	Existing knowledge and information	Public good

Note. From "The Wealth of Networks," by Y. Benkler, 2006.

Various forces such as the state and private enterprises, however, are trying to enclose, or claim proprietary rights, over resources at each of the three levels that Benkler describes. However, the global and open character of the Internet – both as a function of technical design and social practices – constrains the ability to enclose these three layers. Benkler frames the regulatory changes and clashes between the forces that promote an open internet architecture, on the one hand, and those who are pushing for greater levels of enclosure, on the other, as a "battle" over the "institutional ecology" of digitally mediated communication. This framing, in turn, implies these changes or efforts to claim exclusive proprietary rights over the physical, logical and content layers will have important social, cultural and economic effects (Benkler, 2006).

Benkler's typology provides one way of looking at the complexity in the working of the internet and highlights the uniqueness of information resources that sustain each layer. Although many of these layers are inseparable in practice, it is useful to treat them as analytically distinct. Furthermore, Benkler (2006) points out that, essentially, different forces are driving the internet to become a more enclosed space and "there is no

inevitable historical force that drives the technological-economic moment toward an open, diverse, liberal equilibrium. (p. 378)"

Complementing Benkler's mapping of how information is produced and exchanged in a digitally mediated environment, Jonathan Zittrain looks specifically at how a data packet is transmitted across the different layers that make up the internet (see Table 2). His model highlights the five "stops" in the data transmission process that are easily subject to control and regulation. This model says less about the hierarchical layering of the internet but emphasizes the communication process within and between different networks and thus provides a dynamic portrayal of the flow of digital bits.

Zittrain (2003) identifies five "stops": from 1) a source to 2) source ISP through the 3) cloud and handled by the 4) destination ISP and arrive at the 5) destination. These five stops are not only important because they are necessary in the flow of data packets but also because they provide easy points of control. For example, with the implementation of Communications Decency Act (CDA) of 1996, the source of data transfer would be increasingly likely to self-censor when posting content online out of fear of infringing the law. Similarly, the destination of a data transfer, for example, a personal computer or mobile wireless device, can be subject to control by installing filtering software that allow users to monitor, filter and block certain types of content.

Table 2

Jonathan Zittrain's Model of Network Control

Point of Control	Means of Control	Characteristics
Source	Access Control (e.g. passwords); self-censorship	Legally binding (Communication Decency Act, 1996)
Source ISP	As per requested by content Publisher	Limited liability (DMCA and Safe Harbor, 1998)
Destination	PC filtering software	Voluntary, forced installment faces First Amendment challenges
Destination ISP	Blockage	Limited liability

Note. From "Internet Points of Control," by J. Zittrain, 2003, Harvard Law School Research Paper No.54.

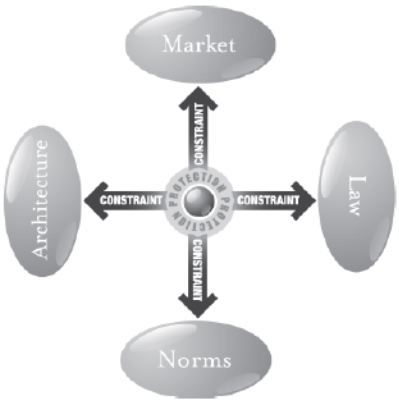
Complementary to the analysis of the key elements, or 'layers' of the internet topology offered by Benkler and Zittrain, Lawrence Lessig (2006) argues that control is a dynamic process that can be arranged and/or implemented in a number of different ways based on: law, social norms, markets and technology, or "code". Lessig (2006) acknowledges the law-like power of technology, in which he argues that the significant governing power of "code", the technical architecture of the Internet, is a form of constitution that structures and constrains social and legal power to the end of protecting fundamental values (p. 4). Other constraining power over the internet arises from market, such as the pricing system, as well as social norms and laws that regulate cyberspace (Lessig, 2006).

Lessig's model suggests that internet regulation is a dynamic process based on the interaction and balance struck at any given place and point in time between law, markets, norms and technical code. This constitutive and dynamic view of control explains the topsy-turvy interplay between different controlling forces that govern the Internet. Moreover, they are interdependent and regulate the internet both directly and indirectly.

His conceptualization of internet control addresses not only the technical architecture of the internet but also the social aspects that comes with it. Recognizing the increasingly salient role of technologists, this framework rethinks the regulation of cyberspace and highlights the significance of code as a newly emerged, seemingly neutral yet powerful regulator.

Figure 1

Lawrence Lessig's Four Modalities of Control



Note. From "Code 2.0," by L. Lessig, 2006.

Craig McTaggart (2003), writing from a legal perspective, provides the most detailed typology of the Internet architecture amongst the four approaches examined here. According to McTaggart, Benkler's three-layer model is too generalized while Lessig's model over-emphasizes on the role of ISPs and code (p. 580). He proposes a four-layer conceptual model of internet control in response (see Table 3). McTaggart's model rests on the fundamental assumption that the internet is not a monolithic technology and that it is essentially, a "co-operative environment". These layers and sublayers provide many points of control but controlling the internet, he argues, is still extremely difficult. However, the fact that Internet is hard to control does not mean it is uncontrollable

(McTaggart, 2003). Moreover, competing jurisdictional claims are always present as factors that further complicate the relationship between layers and sublayers (ibid).

Table 3

Craig McTaggart: Four-Layer Conceptual Model of Internet Architecture

Layers	Sublayers	Main Elements
Content Layer	• Content • Transactions	Data
Application Layer	• Client-side Applications • Server-side Applications	Software
Operational Layer	• Centralized Resources and Functions • Standards and Protocols • ISP Functions	Centralized resources and functions, and ISPs
Physical Layer	• Equipment • Networks	Computer equipment and telecommunication network

Note. From "A Layered Approach to Internet Legal Analysis," by C. McTaggart, 2003, McGill Law Journal.

These four models propose new ways to think about the internet as a technical system that is enabled by a cluster of both physical and virtual elements and material conditions. While these conceptualizations provide different mappings of how the internet works, the common theme is that the internet is not a monolithic technology, and that its smooth functioning relies on a host of different actors. Each element and layer that makes up the internet is subject to its own game rules and prompt different governance issues for different governing bodies. By dissecting the technical architecture and the social forces governing the internet, Lessig (2006), Benkler (2006), McTaggart (2003) and Zittrain (2003) demonstrate the flexibility and malleability of the internet and note that the bottom line is that the internet does not conform to the initial predictions of enthusiasts that it would be an unregulated and anarchic space. Instead, these authors,

each in their own way, argue that the internet has evolved towards a more regulable and controlled medium.

2.2 Internet, State, Market

The characteristics of technical artifacts – the layered architecture of the internet that Benkler, Zittiran, McTaggart and Lessig's conceptual models unveil in particular – highlights the complexity of internet regulation. Internet governance engages many actors and players, as defined by the United Nations Working Group as "the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet" (ITU, 2005). Although internet governance is a collective process that requires cooperation at the international level, nation states still play a crucial, if not an indispensible role.

Much scholarly attention has focused on the role of the state in internet regulation. Although governments rule unwisely in both authoritarian and democratic countries, Wu and Goldsmith (2006) highlight the important role that nation states play in internet governance, stating: "many aspects of the internet that business and individual users take for granted are the product of stable legal environment that only governments provide" (p. 124). Echoing such a perspective, Milton Mueller and Michel van Eeten (2012) argue that there is a need to "bring the state back into [discussions about] Internet governance" (p.722). Given this emphasis on the nation state, as well as private media companies, this section reviews some of the literature on the tension between territorial-bound nation states and the governance of the borderless cyberspace and what the state does to mitigate such conflicts.

The self-governing, anarchist cyberspace envisioned by John Barlow and many others is the antithesis to the territorial-bound traditional nation state. While recognizing the uniqueness of internet as a technical system, Milton Mueller (2010) argues that the internet enables a distinctive global politics wedged between the sovereignty of the territorially-bounded state and non-territorial network space.

In *Network and States*, Mueller examines the origin of rule-making power in internet governance. He argues that internet governance is a new form of polity due to "the internet's transnational scope, its massively increased scale of interaction, its distribution of control, its capacity to facilitate new forms of collective action" (Mueller, 2012, p. 178). The ability to reach more individuals in a significantly shorter span of time distinguishes the internet from other communication technologies. As a result, the internet poses new regulatory challenges and tensions between national and global governance. He proposes a four-quadrant model of internet politics, which include: denationalized liberalism, global governmentality, networked nationalism, and cyber-reactionaries. Each model is characterized by different levels of autonomy of the nation-states authority and the autonomy of global governing bodies in the regulation of internet, and the degree to which control is exerted and the degree of freedom allowed by nation-state (Mueller, 2010). In the denationalized liberalism model, the state exerts the least amount of power and is subordinated completely to global governing bodies, while regulatory problems are solved through empowered internet users by peer-to-peer production and a competitive market (Mueller, 2010). Contrary to the liberalism model is the state-centric and hierarchally-controlled cyber-reactionaries model, in which nation states claim authority over cyberspace. Mueller argues that China exemplifies the cyber-

nationalist model where the state claims national sovereignty over internet regulation with the result that the degree of freedom of Chinese users is limited within state defined boundaries (Mueller, 2010; 2012).

Mueller's four-quadrant model of internet governance showcases the importance of context in determining how a nation state reacts to the challenges brought by the internet. But by capturing the wide range of actions of how state regulates the internet, Mueller's model risks putting too much emphasis on the role of formalized institutions in internet governance, such as nation states, ICANN, and the United Nation's World Summit on the Information Society. As Mueller himself and Eeten (2012) argue, "internet governance" is often ill conceived, as the term often refers to governance that took place in formal institutions while, in fact, it is the private sectors, especially internet intermediaries, and telecommunication companies that have important leverage in standard-setting and policy-making process (e.g. DeNardis, 2012; DeNardis, 2010; Wu, 2006).

Taking account of this critique of state-centrism, Rebecca MacKinnon and Min Jiang's work examines how internet control takes place outside formalized regulatory bodies in authoritarian countries. They examine how authoritarian states interact with and delegate control to market players and the public in order to contain the potentially disruptive social and political implications brought about by the internet. Rebecca MacKinnon coined the term "networked authoritarianism" to conceptualize how authoritarian states co-opt the private sector into controlling the destabilizing effects of the internet (MacKinnon, 2012). Borrowing from Manuel Castell's (1996) concept of the networked society, MacKinnon argues that networked authoritarianism is a new form of

internet-age authoritarianism in which the private sector plays a key role in the state's political authority (MacKinnon, 2012). Authoritarian countries, in this approach, devote considerable resources to "proactively seeding and manipulating the nation's online discourse about domestic and international events" (ibid., p. 198). As a result, private enterprise has become the opaque extension of state power, helping authoritarian regimes to control and manipulate citizens. Within such a context, negative incentives are introduced whereby private companies that fail to censor and monitor their users to the government's satisfaction will put their business interests in danger.

MacKinnon's networked authoritarianism offers a powerful explanation for the survival capacity of contemporary authoritarian countries in the internet age by looking at how states harness the private sector to control the internet. She insightfully points out the power imbalance between states and the private sector as well as the strategic alliances that tie the two together. In this case, the political interests of the state and the economic interests of private businesses are mutually bound together. Unlike Milton Mueller's four quadrants of Internet politics that looks at how authoritarian states maintain legitimacy at the global level, MacKinnon's networked authoritarianism focuses on how states cope with the potential destabilizing consequences of internet from a domestic perspective.

Despite the potential meaningful contributions of this shift in focus from internet governance as global politics to a stress on domestic alliances between the state and private sector, network authoritarianism has been criticized on account of the premises about intentionality the explanation depends on. As Milton Mueller (2012) states: "it is not the best label … the term may attribute too much intentionality to China's approach"

(p. 191). Network authoritarianism portrays the private sector in a powerless and subordinated position and is forced to conform completely to the government's order. As a matter of fact, the relationship between state and private companies is not top-down, total domination but rather a contested process of conflicts, negotiation and struggles. Moreover, MacKinnon's conceptualization does not take internet user's collective bargaining power and agency into account, especially when she states: "controls on political information are nonetheless effective enough that most Chinese are unaware, or have a distorted view, of many issues and events in their own country, let alone the rest of the world" (MacKinnon, 2012, p. 32).

Min Jiang offers a different view on how state legitimacy is maintained through online interaction between state and citizens. Unlike MacKinnon's portrayal of the oppressed, living-in-the-dark internet users, Jiang argues that the heterogeneity and cacophony of public opinion in the Chinese cyberspace is often overlooked in much of the current debates on Chinese Internet (Jiang, 2010). She re-interprets Baogang He's "authoritarian deliberation" in digital communication to describe how government relaxes its grip over political discourse in exchange for its own legitimacy and survival (ibid., p. 4). In this case, the state can no longer fully control public discourse but rather attempts to "talk back" to citizens while giving them limited freedom to speak. Authoritarian deliberation describes the strategies employed by the state to maintain its authoritarian control. Min Jiang argues that, in the Chinese context, there are four main venues where public deliberation takes place, extending from more regulated to less regulated online spaces: central propaganda spaces (government news outlets, government online sites), government-regulated commercial spaces (much of commercial

websites in China), emergent civic spaces (non-commercial, citizen-initiated discussion forums) and international deliberative spaces (Jiang, 2010). The state-citizen interaction implies that control and freedom is no longer a zero sum game, but instead, it is a continuum as the Chinese government tries to reach a fine balance between self-censorship and self-expression.

Min Jiang's approach explains how the Chinese government, in order to secure its own survival, relinquishes certain levels of control over citizen's self-expression in the digital communication environment. This approach recognizes the importance of citizens' online participation and implies that there is at least a modicum of two-way negotiation between governments and citizens in the process of establishing internet controls. As Rebecca MacKinnon (2012) states, there are "a lot more give and take between government and citizens than in a pre-Internet authoritarian state" (p. 198). This also means that governments' control over the Internet is not a static process. Instead, the government learns to allow citizens to speak out while curtailing and predefining the boundaries of tolerated speech. Within this context, the private sector performs a dual role in mediating the interaction between state and citizen. On one hand, the private sector undoubtedly enables more space for public discussion. Thus, as Jiang states, while the "mass media used to be part of the state structure, the commercialization of the Chinese Internet has helped established a platform for public discourse" (Jiang, 2010, p. 17). On the other hand, the importance of commercial interests lies in the fact that they assist the state in strengthening the latter's control of the internet. Again, as Jiang states, "the boundaries of political discourse and actions are largely prescribed by the state and enforced behind the scene with cooperation from Internet companies" (ibid., p. 83). The

proliferation and participation of private sector in internet governance is also manifest in the fact that the Chinese government embraces and incorporates capitalist elements in its internet governance model because economic performance is one source of state legitimacy as well as the cornerstone of the governments long term economic development strategy (Jiang, 2010; Yuezhi, 2008).

Milton Mueller, Rebecca MacKinnon and Min Jiang each have a distinct way of conceptualizing how authoritarian states manage and maintain their legitimacy when faced with the destabilizing potentials of the Internet. Their analyses unfold at different scales. For Milton Mueller, the power battleground takes place at a global level; for Rebecca MacKinnon, the private sector is the command high ground and a key to success for states to maintain their legitimacy; while for Min Jiang, the exercise of control takes place at a more mundane level: state legitimacy is maintained in the day-to-day online communication through interaction with Internet users. While their approaches vary on specific points and complement each other overall, their views towards Chinese internet governance are fundamentally the same: it is state-centric and pragmatic.

2.3 Chinese Internet Control

Mueller, MacKinnon and Jiang all provide valuable insights in thinking about the relationship and interaction between the state, private enterprises and the public when facing the challenge brought by the internet for territorial-bound nation state authorities. As internet control grows into a global norm, cyberspace regulation represents a popular research area, especially in the Chinese context (OpenNet Initiative, 2011). This section reviews some of the existing literature on Chinese internet studies that spans from the early 2000s to the current day. Viewed chronologically, the methods used in censorship

detection, testing and assessment grow more fine-tuned and diverse while the studies that archive the censored content also grow more comprehensive. So, I will organize the existing literature into three categories based on the different research methods used in studying the Chinese internet controls. The first group of literature mainly uses a mixed-method approach to explore the many aspects of the internet control system in China, while the second body of literature employs quantitative methods such as computer testing to reveal various internet controls that are in place in China. The third body of literature is characterized by qualitative method in studying the law and regulations that govern practices and activities on the Chinese internet. Altogether, these studies provide a comprehensive mapping of the control processes that are currently in place on the Chinese cyberspace.

By far, the most comprehensive and interdisciplinary research on the Chinese internet is represented by the work of the OpenNet Initiative, Ronald Deibert and the Citizen's Lab based at the University of Toronto. As early as 2003, Ronald Deibert, employing both technical testing and policy analysis, noticed the trend that the internet has gradually become a more regulable architecture because of pressures from the security and commercial sectors (p. 501). The Chinese internet is an example of such phenomenon. The Chinese censorship regime is composed of self-censorship, legal restraints and punishments and a national firewall at the backbone level that blocks access to undesirable or subversive internet content (Deibert, 2003, p. 512). Starting from 2010, the OpenNet Initiative started to publish yearly reports on the state of internet control and censorship practices around the world. Using the combined method of policy and regulation analysis, technical testing and fieldwork investigation, the OpenNet

Initiative (2010) claims that China has the world's most sophisticated censorship system among all countries and that the Chinese model of internet control features national filtering and blocking system that primarily aims at denying access to unwanted content – an exemplar of the "first generation of control" (p. 4).

Another stream of research on Chinese internet control employs various quantitative methods. Typical methods include manual testing and computer-automated testing and it often requires certain knowledge in computer science to conduct research using these methods of analysis. Jonathan Zittrain and Benjamin Edelman's study is one of the early efforts to examine Chinese internet filtering. They discovered that the censorship efforts were highly contingent and opaque and were often hard to distinguish between an intentional block and a temporary network or server glitch (Zittrain & Edelman, 2003, p. 73). More recent studies also support Zittrain and Edelman's finding about the inconsistent and highly disguised censorship activity on the Chinese internet. For example, Rebecca MacKinnon (2009) used manual testing methods to explore censorship practice on the Chinese blogsphere and found out that different blog service providers approach the task of regulating their users and content with widely varying degrees of enthusiasm and that content censorship is hugely inconsistent as a result. Different sites also differ in their censorship methods. This inconsistency and ambiguity in the operationalization of censorship is supported by a recent study by Joss Wright. Wright's study (2013) shows there is regional variation in filtering in China and thus he argues that the pitfall for many existing internet filtering studies, such as that of the OpenNet Initiative (2011), overlook the heterogeneity within a nation.

As the internet censorship means grow more complicated in China, the complexity of scholarly testing methods has become more nuanced and complicated as well. Keywords testing is also a common testing method used by researchers to determine which kind of content is more likely to be censored on a Chinese website (Crandall, et al., 2013; Ng, 2013; Fu, Chan, & Chau, 2013). These studies demonstrate that censorship on the Chinese internet is highly contingent upon offline politics and that Chinese internet censorship is oriented towards attempting to forestall collective activities that are occurring now rather than criticism about the Party and the country (King, Pan, & Roberst, 2013).

Studies using qualitative methods such as policy research on the law and regulations of the Chinese internet have also emerged from various disciplines such as communication studies and legal studies. Anne Cheung's study (2006) traces the development of Chinese internet regulation and she has also noticed the arbitrariness of law-making and the trend of outsourcing internet control responsibilities to the private sectors. She points out that the cluster of regulations put into place between 1996 and 2000 are repetitive and they all list similar categories of forbidden content (p. 4). Similar studies that focus on the role of private companies have also been done by Ian Weber and Lu Jia (2003). Weber and Jia, for example, explore the motivations behind industry self-regulation rule on the eve of China's accession to the World Trade Organization. They argue that although the motivation behind self-regulation seems innocent, this approach basically downloads the responsibility to control content to individual internet companies (Weber and Jia, 2003, 2007). This line of research highlights the increasingly salient role

that private companies play in the Chinese internet control system and examines the legal and regulatory framework that internet business operates in.

More recently, given the popularization of microblogs among Chinese internet users and the role they played in few recent mass internet incidents, such as the Wenzhou High-speed train crash and Sichuan earthquake in 2008, several studies have focused on Weibo and social network formation and its implication for social mobilization. Two major views have formed with regards to this. One is a relatively optimistic view towards the role that microblogs play in facilitating the formation of networks and social change. For example, studies by Huang and Sun (2014) and Tong and Zuo (2014) recognize Weibo's instrumental role in the development and dissemination of collective action and social movements both online and offline, arguing that Weibo is a "breeding ground for mobilization" (Huang & Sun, 2014, p. 98). Tong and Zuo (2014) claim that Weibo is providing the government with an opportunity to benefit from popular knowledge about local disputes and protests while enhancing its legitimacy by making its punishment of local officials widely known and discussed.

On the other hand, scholars like Jonathan Benney, John Sullivan and Jonathan Hassid provide a more skeptical view towards the role of microblogs and their implications for political change. Through a careful examination of the technical design of microblog, Benney (2013) argues that we should pay more attention to the aesthetics of Weibo rather than viewing it as a mere conduit for information. He argues that Weibo's technical design features create an immersive environment that resonates with the cacophonous spectacle of entertainment while minimizing reasoned debate and discussion (Benney, 2013). As a result, the architecture of the Weibo allows the Chinese

party-state to deliberately manipulate the medium to reduce the risk of activism, controversial uses and social mobilization. Similarly, John Sullivan (2013) argues that claims about the democratic potential of Sina Weibo ought to be treated with caution. For instance, while microblog users may increasingly vent their discontent with various social ills online the government is also growing more adept at harnessing information online to identify and neutralize threatening behavior (Sullivan, 2013).

All of these scholarly works, although different in the research method they employ, demonstrate that when it comes to regulating and controlling the Chinese internet, a myriad of actors such as private enterprises are mobilized. Internet filtering and controls are exerted from technical design to the market and in the legal system. Whether the range of practices that have been disclosed as a result of such research are tantamount to the perfection of internet controls or, on the contrary, a demonstration that the internet continues to help the limits for freedom of speech and social and political mobilization remains an open question.

3 Chapter: Theory and Methodology

Technological determinism, the view that technology is autonomous and self-generating in terms of charting its own course of development, fails to explain why the internet does not bring democracy to China but rather has been harnessed by the state to advance its own agenda: stimulating economic development while exerting control over the flow of information. To fully understand the unique developmental path and internet regulation in China requires us to challenge technological determinism and to take greater account of the social and political forces and contextual factors that are shaping the development of the internet in China. This chapter does this by examining two theoretical frameworks that underpin this thesis. First, I will review two non-deterministic views that help us to interpret the social and political dimensions of the internet: Andrew Feenberg's critical theory of technology, and especially his concept of the double aspect of technology, and Langdon Winner's theory of technological politics. I list some key similarities and common premises in both Winner and Feenberg's theories and the reason why they are relevant to the study of Chinese internet. Secondly, I examine the work by Lawrence Lessig and the OpenNet Initiative, which tackle the vexed question about the regulability of the internet. These two bodies of theoretical work offer a productive framework to interpret the relationship between technology, politics and power.

Winner's theory of technological politics and Feenberg's double aspect of technology share many similarities, especially in relation to three shared underlying assumptions: (1) technology is more than a tool; (2) technology does not determine social outcomes; and (3) technology and politics are closely intertwined and mutually shaping.

Firstly, technology is more than a tool. Both Langdon Winner and Andrew Feenberg argue that technical artifacts are more than collection of tools or rational ways to control nature. Winner, for example, sees technical artifacts as being more than just tools that help us to achieve a certain goal. They also, intentionally and unintentionally, structure how we live our daily lives. This is especially true for large sociotechnical system, which act like laws that structure our life and social activities. Technical arrangements, like legislative acts that establish a framework for public order, define the possibility of what we can and cannot do with any given technology, and influence people's behaviors and perceptions. As Winner (1986) argues, "technologies are ways of building order in our world" (p. 28). Andrew Feenberg (2010) similarly emphasizes the ordering function of technical arrangement. As he states, technology is not only about rationalization and maximizing technical efficiency but also constitutes an environment, "a quality" that "shapes a way of life" (p. 62).

Secondly, technology is not determining, but it does play a decisive role in establishing order in social life. Winner and Feenberg challenge the commonsense notions that technology merely embodies the principles and practices of science. They also reject the idea that technology is completely separated from the society in which they are introduced, used and maintained over time. Both Winner and Feenberg criticize the unquestioned way of conceiving of technical artifacts as neutral and value-free and argue that we should not take any technical artifacts for granted. Winner (1988) uses the term "technological somnambulism" to describe the lack of attention in conceiving the seemingly innocuous yet inherently political technologies. He argues that the idea of technical efficiency and progress became so deeply entrenched during the industrial age

that we tend to overlook the importance of technology in reconstituting the conditions of human existence. As Winner stated a quarter-of-a-century ago, in 1986, it is time to "take technical artifacts seriously" (p. 22). Researchers need to closely examine how the design of technical artifacts can easily be made compatible with certain arrangement of power. Andrew Feenberg (2010) reinforces the idea by arguing that the social dimensions of technology are important sites of enquiry: "no device is too banal for the social study of technology" (p. 74). The unquestioned way of conceiving technical artifacts that make up the fabric of our everyday existence should be abandoned, Winner and Feenberg both argue, in the social studies of technology.

For Winner and Feenberg, technology does not appear suddenly as a finished object, but instead emerges over time. The design and innovation processes are often shaped by the social and political choices that societies make. It is through the analysis of these processes that one can see how certain social groups assert their power over others in defining the meaning of a technology and in relationship to several fundamental questions that accompany the advent of any significant new technology, namely: what is the nature of the problem that is being attended to (definition of the problem and its purpose), how should the technical artifact in question be designed (i.e. as a centralized or a decentralized system), should the technology actually be adopted and, if so, by whom, and lastly, how and who should regulate the new technology once it is deployed?

Essentially, Winner and Feenberg challenge the view that technology just appears fully formed. It is precisely the struggles and compromises between different social groups and the interests they represent that shape a technology's design characteristics and development path. Thus, as Andrew Feenberg (2010) asserts, technologies "offer a

material validation of social order to which it has been perform" (p. 18) and "show traces of past social choices that have been crystalized in standards and material" (p. 75).

Thirdly, technology and politics are closely intertwined and mutually shaping. Given the emphasis on the technical artifacts themselves and the social forces that shape their development, both Langdon Winner and Andrew Feenberg argue that the politics of technology cannot be separated from the politics of the society in which they are situated and that "struggles over technology thus resemble political struggles in important respects, and in fact in the contemporary world, struggles over technology are often the most important political struggles" (Feenberg, 2010, p. 80). On the one hand, the design and development of a technology is heavily influenced by existing technical choices and political struggles. On the other hand, the character of technical artifacts can prescribe how power is organized. This latter point is especially obvious in Langdon Winner's example of a highly centralized nuclear power plant that needs centralized and hierarchical control versus a de-centralized solar energy system that is highly compatible with more dispersed forms of control.

Furthermore, both Winner and Feenberg see that the relationship between technology and politics as being closely enmeshed together. Langdon Winner argues that the rationalizing logic of technological development has been exported without carefully considering its impact on politics (Winner, 1980, 1977, 1986). For example, the desire for power and conquest now become the guiding impulse of politics (Winner, 1986, p. 20). Andrew Feenberg also sees that technical politics are an important but often overlooked site of power struggles. He argues that most technological choices are privately made and are protected by property rights and technocratic ideology and thus many interests and

concerns are excluded in the final design of technology (Feenberg, 2010). As a result, opening technology to a wider range of participation is a crucial step towards democratization and emancipation (ibid.,).

3.1 Double Aspect Theory

Andrew Feenberg's double aspect theory of technology is examined here because it provides a way of interpreting technology that takes the larger social and historical context into consideration. Feenberg (2010) contends that there are two crucial hermeneutic dimensions in conceiving a technology: functional rationality and social meanings. These two intertwined dimensions of technology each reveal a specific contextualization. Functional rationality, which decontextualizes the technology from its social setting and only views its ability to achieve a certain goal, is how a technical object is most commonly conceived (Feenberg, 2010). For example, social institutions such as labs and research organization and engineers primarily focus on the design of the technical object and aim to improve its capability to meet certain needs.

The social meaning of technology, on the other hand, is not fixed and hinges upon different positions occupied by social groups. The social meaning of a technology can shift over the course of technological development. For example, in the late nineteenth century, bicycles were conceived as both a competitive sport for "young men of means and nerve" (Pinch & Bijker, 1984). The meaning of bicycle, therefore, was primarily conceived of in terms of sporting, masculine and entertainment values. However, women, who were forbidden from riding a bicycle, argued that it was the only a means of transportation to reach the church on Sunday. The meaning of bicycle subsequently shifted from entertainment values to utilitarian ones. The change in meaning after the

contest of interpretation also led to changes in the design of the bicycle – from the rule of speed to the rule of speed as just one priority among other considerations, including functional ones and social norms related to gender (ibid). This is an example of how different social groups interpret the same technical artifact differently and how such differences can lead to changes in how the technical artifact is designed.

Although functional rationality and social meanings seem like two ontologically distinct ways to interpret a technology, they are inextricably intertwined. Andrew Feenberg (2010) argues that we need to pay closer attention to the cultural horizon that gives rise to such ways of thinking: it is the fetishism of technological rationality and pursuit of efficiency in modern capitalist society that constrains our interpretation of technology to its functionality, he asserts. This creates the "bias" of technology, by which he means that we most often see it as neutral while tending to neglect the social meaning of technology – a stance that largely stems from hegemony in modern capitalist society which pursues the maximization of technical efficiency (ibid.,).

Andrew Feenberg's double theory of technology makes explicit the often-unquestioned role of hegemony in shaping our view towards technology and re-asserts the importance of social context and order in shaping the path of technological development. The double aspect theory of technology provides a critique of the pursuit of "technological rationality" in capitalist societies that leads to an ahistorical conception of technology – a mere instance of the rational control of nature. This conception, in turn, helps to further legitimize technology. The double aspect theory serves as a reminder of how functional rationality and social meanings are actually closely intertwined, dependent on and legitimized by one another. Therefore, for social change to take place,

radical technical as well as political changes are needed. According to the double aspect of technology, it is not only the developmental process of a technology that needs to be examined in terms of its influence on social order but also the larger social hegemony that gives technologies their meaning and which bias our common perceptions of technology. Thus the double aspect theory of technology provides a way to conceive of the relationship between technology and society that is both historical and contextual, and is as much concerned with the functional and technical specificity of technology as with its symbolic dimensions and meaning.

3.2 Theory of Technological Politics

Compared to the double aspect theory of technology, Langdon Winner's theory of technological politics puts greater emphasis on technical artifacts themselves. Winner (1980) argues that although the social, political context within which certain technological artifacts emerge is important, the technological artifacts themselves can have political properties. In particular, Winner claims that there are two ways that technical artifacts can embody power and authority.

One way that technical artifacts can embody forms of power lies in the decision of whether a certain technology is selected as a way of settling an issue in a particular community (Winner, 1980). Because technologies are ways of building order in our world and contain possibilities for many different ways of ordering human activity (ibid., p. 127), the social group that makes the structuring decisions exercises power and influence over others. This is true especially when a technology is not widely adopted and the meaning of a technology is not settled. Therefore, to decide whether to choose a certain tool is to think in time and to imagine change (Nye, 2006). Judgments about

technology are often made on narrow grounds because various social groups have different levels of access to the decision-making process and therefore have unequal levels of awareness.

If the yes/no question in deciding the adoption of a certain technology is a straightforward process where power can be exerted, a more intractable and invisible way for a technical artifact to embody power and authority is through its design features. Different technology designs require different social and material conditions to be created and met in order for the technology to operate. Inspired by Lewis Mumford's *Authoritarian and Democratic Technics* (1964), Langdon Winner discusses two types of technologies that have recurrently existed side by side: centralized and decentralized. A centralized technology is system-centered, immensely powerful but inherently unstable, whereas a decentralized technology is more human-centered and relatively weak, but resourceful and durable. Different design features of technical artifacts and technical system require different social environment and material conditions to be structured in a particular way in order to keep the devices running. Consequently, these immanent characteristics of technology design institutionalize fundamentally different patterns of power and authority and, as such, these arrangements are inseparable from politics (Winner, 1986).

The emergence of the internet on different university campus exemplifies these two variations in design. At the University of Chicago, the web was initially designed in a way that allowed anyone to log on freely and anonymously. At Harvard University, in contrast, the internet was initially designed to only allow a registered individual to log on using a registered machine and after accepting the university's user agreement policy

(Lessig, 2006). The results from these two basic approaches to the internet resulted, in essence, to very different internets: at the University of Chicago, it is more user-centric and minimizes the collection of personally identifiable information whereas at Harvard it is more controlled and maximizes the collection of personal information. These variations in technical design also imply different conceptions of how the internet is controlled on two university campuses. Although the centralized, hierarchical control model of Harvard contradicts the values of liberty, justice or equality, in the "common sense" view of technology that often seem to carry the day, basic decisions about the internet were taken in a manner that was largely separate from politics. Langdon Winner (1980) argues, in contrast, that such moments where choices over technological design come to a head must not be over-looked because technology structures the condition of human activity and social life. The conditions just described with respect to the contrasting paths of internet development at the University of Chicago and Harvard University are symptomatic of processes that take place regularly when it comes to the politics of technology across societies writ large.

Winner provides a novel framework in analyzing how technology embodies forms of power and authority. His approach, although centered on the "things" themselves, stresses both the external working conditions of the technology and the relationships of authority and subordination that arise independently of all social organizations within a certain technical system (Winner, 1980).

Langdon Winner and Andrew Feenberg's non-deterministic views of technology take the social, historical context into consideration and highlight how technical artifacts develop through a dynamic process that is embroiled in the political condition of the

society. Both Winner and Feenberg have shown that by carefully reading the character of technical artifacts, and by examining how a certain technology develops over time, one will gain important insight of how social conditions and cultural choices shape the developmental process of technology. The upshot of their approaches is that technology can be seen as neither neutral nor determining: instead, it is deeply embedded in the conditions of politics and is socially constructed. These two theoretical perspectives encourage us to take the larger social economic context in the studying of the internet in China.

3.3 Models of Internet Controls

Lawrence Lessig explicitly builds on Winner's work to develop an understanding of the four main modalities that render the internet more or less regulable. In *Code 2.0*, Lessig (2006) argues that the internet is becoming a more regulable space, contrary to the initial end-to-end design of the network and the utopian views of many who seemed to think of it as an inherently unregulable technology. Similar to Langdon Winner's argument, Lessig argues that the technical architecture of the internet is a form of constitution that structures and constrains social and legal power in ways that, depending on the decisions taken, will serve to either protect fundamental values, or erode them (p. 4). The law like power of technical design, Lessig argues, means that we have to take a step back and understand how regulation works in cyberspace.

In essence, Lessig argues there are four things that regulate cyberspace: the technical architecture (code), norms, markets and laws. Law is the most common and traditional regulator. Market rules through pricing mechanism or market outlooks. For example, if the price of cigarettes is low, then it encourages smoking. Social and cultural

norms also regulate what types of behaviors are acceptable. Lastly, architecture, or code, is an increasingly salient regulator, with rules and constraints being built in the software and hardware that comprise the internet. For example, access to certain services and websites are denied unless you sign in with a password. These codes are written by engineers and embed certain values. Lessig emphasizes that these four modalities do not rule in isolation from one another but interact with and affect one another. In sum, internet regulation is a dynamic process based on the interaction and balance struck at any given place and point in time between law, markets, norms and technical code.

This constitutive and dynamic view of cyberspace control explains the topsy-turvy interplay between different controlling forces that govern the internet. Moreover, they are interdependent and regulate the internet directly and indirectly. Lessig's conceptualization of internet control addresses not only the technical architecture of the internet but also the social aspects that comes with it. Recognizing the increasingly salient role of technologists, Lessig expands our understanding of regulation from traditional institutions to codes in the digital communication environment.

Employing interdisciplinary research methods, such as computer testing, policy analysis and field research, the OpenNet Initiative conducts tests on internet filtering and blocking in various regions across the world. Based on their empirical studies, especially in their study on the internet in Russia (RUNET), Ron Deibert and Rafal Rohozinski (2011), outline three different generations of internet controls that have evolved over time. As shown in Table 6 below, the first generation of internet controls mainly focused on denying access to web content. Chinese-style internet filtering, is one of the best example of this first generation of internet controls. However, they argue that while internet

filtering and blocking have been identified in various countries, internet controls are increasingly being exercised in more subtle, hidden and temporally specific forms. They refer to these latter efforts as exemplifying the rise of second and third generations of internet control (Deibert & Rohozinski, p. 17). Second generation internet controls involve legal and normative pressures to censor and otherwise block or filter internet content. In these approaches, the state is the main actor who decides what types of content are "acceptable" and in terms of expanding the use of defamation and slander laws as a means of deterring users from expressing themselves freely on the internet. National security concerns are employed as justification for blocking. The third generation control is the most sophisticated and multidimensional approach of all. Through the creation of national cyberzones and enhanced government surveillance, this generation of control aims to incite cognitive changes in internet users rather than hard blocking and denying access.

Table 4

OpenNet Initiative: Internet Control Models

Generation	Main Control Practices	Examples	Characteristics
First Generation Control	Denying access, blocking and filtering, policing and surveillance	Cyber Cafes, ISPs	Overt
Second Generation Control	Construction of a legal and normative environment to justify censorship	Strict registration policy; defamation laws; magnifying national security concerns; DDoS attack; "in-time" blocking	Both Overt and Covert
Third Generation Control	Strong national informational space; creation of national cyberzones	User surveillance and data mining; dissemination of prepackaged propaganda	Highly sophisticated and multidimensional

Note. From "Access Controlled," by R. Deibert and R. Rohozinski, 2011.

These three generations of control capture the long-term evolution and drastic shifts in the control mechanism that governments have deployed to exercise control of the internet. The general trajectory has been from crude and harsh technological means of filtering and blocking content (first generation) to the use of less apparent and non-technological means such as the law to cultivate an environment in which both internet services providers and internet users assume a greater role in policing internet content and self-censoring (second generation). In the third generation of controls, states play a more active role in shaping the communications environment through the use of propaganda and by encouraging patriotic hacking as well as the assertion of strong national identity within the realm of cyberspace. Overall, these three generations of control indicate that internet controls are becoming more multidimensional and subtle. They also highlight how governments are offloading policing activities onto Internet Service Providers. This conceptualization of the evolution of internet controls over time also supports Lessig's contention that the internet is prone to regulation and that regulation comes in various forms, ranging from law to technical arrangement and norms that often rely on the cooperation of private actors. Together, these theoretical explanations offer useful conceptual tools to study how the internet has steadily shifted from its initial design according to end-to-end principles that minimized control over information flows into a highly centralized and tightly controlled technical system, especially in China but to varying degrees in other countries around the world.

3.4 Research Methodology

The internet is not a single technology. It is a system that comprises a host of different actors, ranging from physical infrastructure, network intermediaries to software

programs and code. In this thesis, the internet is conceived of as a large sociotechnical system which consists not only of hardware, but also of legal, corporate and political-economic elements (Edwards, 2003). Based on this understanding, I employ Paul Edwards' multi-scalar method to study the internet in China. Paul Edwards emphasizes the importance of scale in understanding the complex and large-scale infrastructures that constitutes the modern society. By reviewing infrastructure across different scales of force, time and social organization, we discover different stories about our 'object of analysis'. The multi-scalar method is advantageous in untangling the complexity and socially constructed nature of what, at first blush, often appear to be the seamless, natural and unobtrusive character of the infrastructural technologies that constitute the background of modernity (Edwards, 2003). Edwards' multi-scalar method helps to yield a fuller understanding of the vulnerability and fragility of the infrastructure that one cannot see if only focusing on technological momentum.

Among the three different scales that Edwards uses in his study of infrastructure (force, time and social organization), the scale of social organization is particularly relevant to the study of the Chinese internet. Examining infrastructures on different social organizational scales illustrates that infrastructural technologies exist simultaneously within smaller temporal and social groups, such as user groups, at the level of institutions and in the historical progression of the country's communication technology and infrastructure.

Edwards borrowed the concepts of scale and social organization at the heart of his analysis from Thomas Misa (1988, 1994), and adopted them to his study of infrastructure.

As Edwards and Misa both note, the social scale of complex infrastructural technologies needs to be examined across three key levels of analysis:

- Micro: individuals, small groups; generally short-term
- Meso: institutions, e.g. corporations and standard-setting bodies, generally enduring over decades or longer
- Macro: large systems and structures, such as political economies and some governments, enduring over many decades or centuries

Edwards (2003) argues that macro scale analysis focuses on the functions that are assigned to a particular technical system rather than technology itself: "particular technologies and systems are less important than the functions they fulfill", is how he puts it (p. 221). Thus infrastructures become, not a rigid background of overpowering technologies, but a constantly changing social response to problems of material production, communication, information, and control (p. 222). Micro-scale analysis looks at how individuals and small, spontaneously organized social groups exert agency over the technical infrastructure while meso scale analysis looks at the infrastructure itself.

3.4.1 Macro-level analysis

At the macro-level, the analysis in this thesis contextualizes the internet within the larger political economy of China at the turn of the 21st century. Historical government policies, key regulatory texts, legal texts, key statements issued by the government ministries involved in media regulation, such as *The Internet in China* White Paper (IOSC, 2010), economic development plans published by the Party and which prioritize the use of information and communication technology as the driver for innovation and the country's industrialization agenda are used to outline the contours of the internet

control system and the place of the internet within the large political economy of China. Other than these government texts, early scholarly work on the Chinese internet will also be critically examined, such as the study by Mueller and Tan (1997) and Taubman (1998).

3.4.2 Meso-level analysis

Analysis at this level focuses on the infrastructure itself. From the level of the institutions, I will conduct a systematic review of the published policy and regulatory documents pertaining to the topic of internet regulability and control. This includes an overview of the mandate of different organizations such as the State Administration of Radio, Film and Television (SARFT), the Ministry of Information Industry (MII) and the Public Security Bureau (PSB), as well as the existing laws and regulatory oversight that make up the system of internet governance in China. Authoritative English translation of the media laws in China are used such as the *Chinese Media Law Database* and the World Intellectual Property Organization's law depository on Chinese media regulation. Other primary sources, government policies and the mandates of government organizations listed on the English version of the People's Republic of China's website, the annual *Statistical Report on Internet* released by the China Internet Network Information Center (CNNIC), the annual *Blue Book of Law* and the *Annual Report* on the Development of New Media in China published by the Chinese Academy of Social Science (CASS), are also used extensively.

Given the overlap between the regulatory roles of different organizations, and the arbitrariness in the Chinese internet law making, existing scholarly studies that probe into the legal and regulatory framework of Chinese internet regulation will also inform the research process and provide a useful bibliography. Several studies along these lines

stand out, such as Lokman Tsui's (2001) thesis on Chinese internet control, Henry Hu's (2011) study of the political economy of ISP governance in China, Fan Dong's (2012) overview of the Chinese government's layered internet control mechanism, as well as studies by the legal scholars Jyh-An Lee (2012) and Anne S.Y. Cheung (2006), respectively, on microblogging regulation and content regulation. These studies outline the current regulatory framework and pinpoint the relevant laws and organizations that are very informative to this research.

3.4.3 Micro-level analysis

For the micro-level analysis, which will focus on the technical design of Weibo from users' perspective, I will employ observation techniques to immerse myself in the constructed online space. Analysis at this level focuses on the legally binding, click-through contracts that Weibo users have to consent to when they first sign up to the service. According to Sina Weibo, by clicking "I agree", users consent to three contracts: *Sina Terms of Service*, *Sina Weibo Terms of Service* and *Sina Weibo Community Guidelines* (Sina, 2013). These texts are important as they not only set the condition of participation but also "act as legal agreements that lay claims to the institutional power of the state to guarantee and enforce them" (Stein, 2013, p. 361). I will examine the content in these user contracts, with a special focus on the statements of the company's liability over violations and to the company's statements regarding its legal obligations under the official legal framework that regulates cyberspace in China. As Laura Stein (2013) argues: "these terms are part of the sociotechnical arrangements surrounding platform users and invoke legal claims on which platform owners and users can rely in the event of conflicts" (p. 354).

Other rules such as the *Weibo Community Regulation* that regulate and set the boundaries of what is permitted and not permitted on Weibo will be examined. Related is the rules and Weibo Scoring system: this credit mechanism helps Weibo users to build trust/credibility online while encouraging participation on Weibo, thereby helping the company to maximize its profit.

4 Chapter: The Internet in China: Breaks and Continuities

> History shows a typical progression of information technologies: from somebody's hobby to somebody's industry; from jury-rigged contraption to slick production marvel; from a freely accessible channel to one strictly controlled by a single corporation or cartel - from open to closed system. – Tim Wu, *The Master Switch*

As Langdon Winner (1987), Andrew Feenberg (2010) and Tim Wu (2006) have all argued, a technology often develops within a specific sociopolitical context and follows a path that is relatively flexible at the outset but which becomes increasingly calcified after this initial period of openness and 'flexible interpretation' (Feenberg, 2010). The development, commercialization and use of the internet in China exemplifies this reality.

This chapter provides a historical analysis of internet development in China by focusing on the political, economic and institutional settings in its early period of development (1987-1996). It is argued here that the fragmentation of regulatory authorities, nationalism and the commercial logic are three key characteristics that prevail throughout this period of development. By re-visiting the early period of the Chinese internet development, this chapter offers insight into the formation of the government's instrumental and nation-centric view towards the internet, as identified by many scholars (Meng, 2010; Jiang, 2010; Mueller, 2010).

As Kalathil and Boas (2003) argue, a reconsideration of the historical root of internet development is essential in contextualizing and understanding current policy as the internet is often the "outgrowth of the country's older regulatory regimes for traditional media and telecommunications" (p. 5). This historical and macro perspective that focuses on large sociotechnical systems and structures that have endured over

decades is advantageous in unveiling the functions that have been assigned to a particular technical system rather than simply focusing on the technology itself. This shift in focus from the functions of technology to a wider examination of how persistent social needs and institutional arrangements subtly shape the role and character of technology emphasizes the importance of social context, historical continuity and political economy in deciding what a technology will become.

In examining internet governance in authoritarian countries such as China, Cuba, Singapore, Vietnam and Burma, Kalathil and Boas (2003) noted that "in such [authoritarian] countries, early experimentation with the Internet usually occurs in the scientific or academic sector, but the central government is generally the major player in any Internet development beyond the experimental level" (p. 5). Given the central role of the government in building, regulating and fostering preferred uses of networks, this chapter examines key documents issued by various governmental organizations such as the Chinese Communist Party's *Five-Year Plans* for information and communication technology (ICT) development, as well as regulatory decrees published by the tangle of specialized internet governance committees and bureaucratic players that articulate the 'rules of the road' for the ownership, development, use and regulation of the internet in China.

4.1 The Internet in China

Similar to many other countries, China's early effort to develop the interent was centered on research and the scholarly exchange of information (Liang & Lu, 2010, p. 104; Tan, Mueller, & Foster, 1997). The country's first computer network, China Academic Network (CAnet), was established in 1987. It was enabled and operationalized

as part of the government's 863 Plan to foster hi-tech research and development, and to accelerate China's industrialization process (China.org). In 1987, Qian Tianbai, a professor from the Chinese Academy of Science (CAS) sent the first email message from China to Germany: "Across the Great Wall, we can reach every corner in the world", he exclaimed (CNNIC, 2012). Seven years later in 1994, China connected its first international dedicated line to the internet and became the 71st country to register onto the global computer network, operating under the country-level domain name CN (Lu et al., 2002). As shown in Table 5, some of the country's early international internet connections were built for educational and research purposes by univeristies, academic and research institutions. For example, China Education and Research Network (CERNET), funded by the Chinese government through the State Planning Commission, China's National Science Foundation, and the State Education Commission, developed the country's first national network, linking up to more than 200 universities through eight regional centers (Tan, Mueller, & Foster, 1997). Research and educational networks, like China Science and Technology Network and China Education and Research Network, also constitute a significant portion of the country's bandwidth.

Table 5

Ownership and Usage of Major Networks in China

Name	Organizations in charge	User
China Education and Research Network	Ministry of Education	School and Research Institutes
China Science and Technology Network	Chinese Academy of Sciences	Scientific Research Institutes, government enterprises and state enterprises
ChinaNet	China Telecom (MII)	Public
ChinaGBN	Ji Tong (MII, former MEI)	Public
UNINet	China Unicom	Small Medium Enterprises
CNCNet	China Netcom	

Table 6

1997-2003 Bandwidth Allocations of Chinese Internet

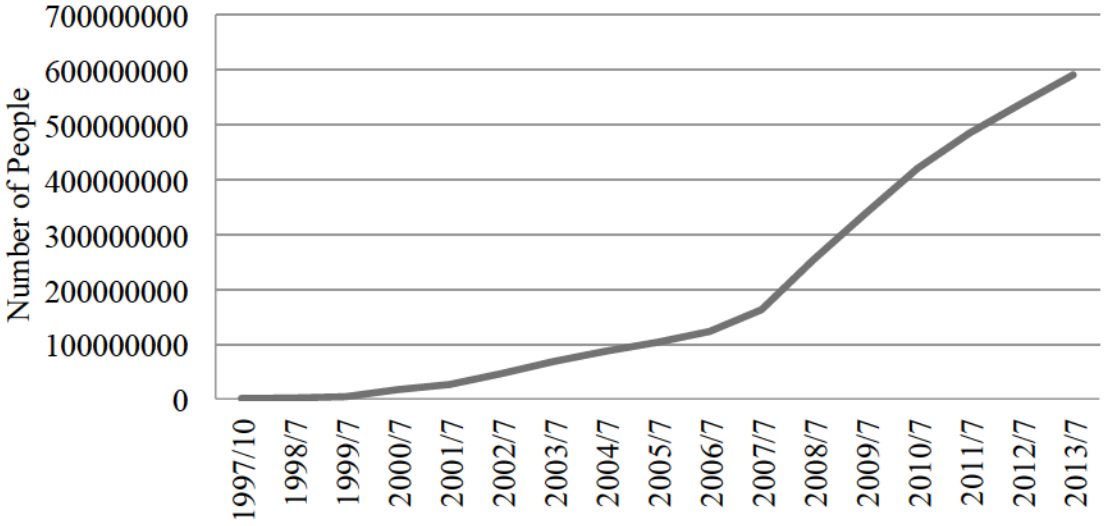
Year	China Science and Technology Network	ChinaNet	China Education and Research Network	China GBN	UNINet	CNCNet	Total
Oct-97	2.1	18.8	2.3	2.3			25.4
Jul-98	2.1	78.0	2.3	2.3			84.6
Jan-99	4.0	123.0	8.0	8.3			143.3
Jul-99	8.0	195.0	8.0	18.0	12.0		241
Jul-00	10.0	711.0	12.0	69.0	55.0	377.0	1234
Jan-01	55.0	1953.0	117.0	148.0	55.0	377.0	2799
Jul-01	55.0	2387.0	117.0	151.0	100.0	355.0	3257
Jan-02	55.0	6032.0	257.5	168.0	418.0	465.0	7597.5
Jul-02	55.0	6452.0	257.5		693.0	2870.0	10576.5
Jan-03	55.0	5147.0	259.0		1093.0	2469.0	9380
Jul-03	55.0	10959.0	324.0		1435.0	2112.0	18599

Note. Author's compilation from CNNIC semi-annual reports, 1997-2003.

The internet users in China has also grown exponentially over last two and half decades. As Figure 2 shows, the number of internet users grew from merely 620,000 in 1997, to approximately 591 millions in 2013 (44.1% of China's total population), which makes China the biggest internet population in the world. The most significant growth took place between 2007 and 2008, with the number of internet users nearly doubled within a year's time, from 137 million to 210 million.

Figure 2

Growth of Internet Users in China



Note. Author's compilation from CNNIC reports, 1997-2013

The range of internet uses has also expanded well beyond email to a wide variety of social, economic and political uses. As Table 7 illustrates, in the early stage (1999-2005), email and search engines[3] were the most commonly used applications online (as reported by users). While the porportion of search engines usage amongst the surveyed population has remained stable over time, email use as well as file transfer and downloading have fallen drastically, from 90.9 percent to 41.8 percent with respect to email and from 59.6 percent of uses to an unspecified amount, respectively. In stark contrast, however, the social and entertainment functions of the internet – chatting and online gaming, in particular – have surged. The percentage of users indicating that they chat online has soared from 29.2 percent in 1999 to 84.2 percent in July 2013, while those identifying internet gaming as a regular activity also surged from 15.8 percent to

[3] The categories used in the CNNIC reports are inconsistent over time from 1997 to 2013, reflecting the changes taking place in internet usage. For example, the category named "file upload and download" was the third most used applications whereas it ceased to exist in the 2013 report.

58.5 percent over the same period of time. At the same time that this tremendous growth in internet penetration and the range of uses has occurred.

Table 7

1999-2012 Most Commonly Used Web Applications

Year	Search engine	Email	File Download/Upload	Chat	Gaming
Jul-99	65.5	90.9	59.6	29.2	15.8
Jul-00	55.9	87.7	50.7	38.8	17.7
Jul-01	51.3	74.9	43.9	21.9	15.8
Jul-02	63.8	92.9	51	45.5	18.6
Jul-03	70	91.8	43	45.4	18.2
Jul-04	64.4	84.3	38.2	40.2	15.9
Jul-05	64.5	91.3	25.8	44.9	23.4
Jul-06	66.3	64.7	33.9	42.7	31.8
Jul-07	74.8	55.4	-	69.8	47
Jul-08	69.2	62.6	-	77.2	58.3
Jul-09	69.4	55.4	-	72.2	64.2
Jul-10	76.3	56.5	-	72.4	70.5
Jul-11	79.6	51.9	-	79.4	64.2
Jul-12	79.7	48.1	-	82.8	61.6
Jul-13	79.6	41.8	-	84.2	58.5

Note. Author's compilation from CNNIC report, 1999-2013

4.2 A Tentative Freedom Arises Out of Early Administrative Fragmentation

Censorship and political control loom large in many studies on the Chinese internet. Journalistic accounts often arrive at a similar picture of China's heavily regulated internet and how Chinese internet users groan under the oppressive weight of the Chinese government. A common pitfall of these studies, however, is that there is little mention of the historical background of internet development in China. Laurl Paltemma and Juha Vuori (2009), for example, argue that a longer historical perspective is needed to grasp the logic that has driven Chinese internet control – something that is largely missing in much of the contemporary literature on the subject (p. 3). Even when such

factors are given their due, the development of the internet is either presented in a very brief summary or is framed as having been a tightly controlled technology since its inception.

Givens and MacDonald (2013), for example, claim that the state has, from the day the first modem was connected, largely been able to maintain firm control over political uses of the internet. However, when one revisits the initial phase of internet development in China, especially from 1987 to 1996, it reveals a different picture. In fact, the internet enjoyed a period of relative freedom when it was first introduced into the country. The Chinese government took a more or less "laissez faire" approach to the regulation of the internet in this early period (Harwit & Clark, 2006). In this stage of development, conflict between different bureaucratic/state institutions was the main character.

As Table 5 showed previously, China's internet initiatives are mainly backed by various technical experts and educational institutions such as the Ministry of Post and Telecommunications (MPT), Ministry of Electronics Industry (MEI), State Education Commission (SEC) and Chinese Academy of Science (CAS). These organizations are on the same level in the government hierarchy, with roughly similar powers (Mueller & Tan, 1997, p. 97). The lack of a single powerful organization overseeing the initial phase of internet development led to fierce competition between these organizations, especially between the MPT and MEI. As a result, this inter-ministerial competition created a period of relative freedom in the early era of internet development before the government clamped down on the internet in 1996 (Harwit & Clark, 2006; Mueller & Tan, 1997; Damm & Thomas, 2006, p. 2; Tan, 1995).

Prior to the introduction of the internet in China, the Ministry of Post and Telecommunications was the key regulator and operator in China's telecommunication sector. This traditional regulatory authority in telecommunication strived to continue its powerful position in the age of the internet. In 1993, under the leadership of newly appointed minister Wu Jichuan, the Ministry of Post and Telecommunications (MPT), seized the opportunity to benefit from the commercial value of the internet by building its own commercial packet-data network, CHINAPAC – the largest commercial data network in China at the time. It ran on equipment from Nortel and Newbridge, while the United States-based telecommunications company Sprint provided assistance with respect to international links and domestic planning (Mueller & Tan, 1997, p. 87). As a life-long telecommunication bureaucrat, Minister Wu was known for his ambition to establish firm control over the telecom sector. Indeed, he actively advocated for the MPT's regulatory authority over all areas of voice and data communication (Harwit & Clark, 2006). He was also a firm believer of the technology's potential in national development, observing that "China's telecommunications construction can leap over some development stages and technical levels which Western countries had gone through and directly adopt highly efficient new technology and equipment" (Reuters, cited in Chu, 1997). With the construction of CHINAPAC, and lines leased to the State Education Commission's Chinese Education and Research Network, the MPT functioned not only as a regulator but also as an operator for the country's largest commercial data network and its first nation-wide network.

Other ministers and ministries, however, saw the Ministry of Posts and Telecommunications as limiting demand for high-speed communication. The State

Council responded to this perceived situation, for instance, by attempting to instill competition in the telecommunication sector. In 1992, the State Council joined the effort to promote greater competition when it combined with the Ministry of Electronic Industries to propose the creation of Lian Tong (China Unicom) to "fully develop the potential of China's dedicated networks" together with the Ministry of Electric Power and the Ministry of Railways (Tan, 1995). Lian Tong (China Unicom) interconnected these ministries' private networks and began to compete with the MPT in long-distance communications. The MEI also created another company, Ji Tong, a satellite-based telecommunication network, with the People's Liberation Army as its major shareholder. Ji Tong was in charge of the country's e-government project that aimed to digitize and connect the state economic, financial, medical and governmental networks. These initiatives were the cornerstones of the national scale e-government and digitalization project called the Golden Projects. Lian Tong and Ji Tong, in short, created competition in the long-distance communication sector, thereby mounting a significant challenge to the Ministry of Post and Telecommunications monopoly (He, 1997).

Although early competition was largely backed by government organizations, control over the internet, especially control over internet content, was less stringent and systematic relative to current standards. The fragmentation of authority not only spawned some competition in the Chinese telecommunications market but also created greater space for freedom to experiment and to speak openly across the internet. The fact that computer networking did not fall clearly and unambiguously into the jurisdiction of any specific ministry or department was an important contributing factor in this state of affairs. As a result, many uncoordinated, centralized, and in some respects competing

initiatives emerged in the early 1990s (Mueller & Tan, 1997, p. 82). Within this context, the Central Propaganda Department's firm grip on domestic information providers and network infrastructures proved to be ineffective in maintaining control over information passing through these networks.

However, it was not long before the growth in the internet user population, coupled with the circulation of anti-government information from overseas, alerted the Chinese government to the potential perils of a weakly regulated and relatively uncontrolled internet. Already by 1996, a series of network regulations were implemented that established the foundation of current internet regulations in China. Another raft of regulations that remain determinant to this day was also promulgated on the eve of China's accession to the World Trade Organization in 2000. A bureaucratic re-organization in 1998 that resulted in the Ministry of Posts and Telecommunications and Ministry of Electronic Industries being unified into the newly created Ministry of Information Industry also signaled the end of bureaucratic balkanization and struck another blow in favour of tightening the government's clamp on the internet.

4.3 Perpetuation of Nationalism

The development of the telecommunications industry in China carries the scars of many anti-colonial and anti-imperial struggles. Given that the country's technical backwardness is one of the reasons for its defeats in the late Qing Dynasty, recent developments in the telecommunications industry have been seen as crucial achievements in the country's national development and a boost to national pride. The logic of internet development in China unequivocally bears the imprint of such nationalistic themes and outlook. Moreover, given that the internet was introduced in the middle of the nation's

industrialization and informationization program, its function is primarily conceived of in instrumentalist terms by the Party as a means of leapfrogging development and reviving national pride. In other words, the internet has carried the weight of helping to "revive the middle kingdom". In addition, the nationalist theme has been consistently reflected in the government's justification for and logic of internet regulation and network control. Last but not least, nationalism is also a prominent theme in online communication and cultural expression.

Looking back at China's telecommunication development from the mid 1870s to the early 1990s, Zhou He (1997) noted that the persistent struggle for national sovereignty in telecommunications is one reoccurring theme during the long and rough development of China's telecommunications (p. 55). In reaction to the danger of colonization, Qing officials launched the "Self-Strengthening Movement" (洋务运动), which advocated that China embrace advanced technologies from the West while discarding the values, ideology, and political cultural systems that lay at the roots of the technologies. Such an instrumental view towards technology was perhaps best exemplified in two maxims: "learning the superior technology of the barbarians in order to control them" (师夷长技以制夷) and "Chinese learning as substance, Western learning for practical use" (中体西用). Essentially, such thinking was a manifestation of Andrew Feenberg's (2010) idea that technology can be interpreted merely according to the instrumental values of productivity and efficiency and in a decontextualized way, with little attention given to the culture that sustains such development and the morals and values that shape its impact, diffusion and use (Chu & Cheng, 2011, p. 28; Tsui, 2007).

Since the end of Maoist China, China has introduced an ever-expanding role for the market in its planned economy. Simultaneously, the government launched the *Four Modernization* projects in agriculture, defense, science and technology, respectively. Wai-Chi Chu and Chung-Tai Cheng (2011) and Xiudian Dai (2000) observe that the distinctive reformist context set by these overlapping goals is crucial to understanding the internet in China, with the country trying to ride the double juggernaut of industrialization and digitization at the same time. Despite its social and cultural implications, the internet, first and foremost, performs a crucial nationalistic role in assisting the ruling Party to achieve its goal of washing away the century-old humiliation from its past defeats while trying to improve China's position in the global economic and political order. The technical efficiency of the internet is endorsed by various generations of leadership in helping the country to "catch up with the West" and to "revive the Middle Kingdom". Alvin Toffler's theory of Third Wave is especially popular amongst academics and politicians who believe that taking advantage of the global communications revolutions will allow developing countries to jump-start economic development (Dai, 2003, p. 9; Damm, 2007, p. 279). In particular, the idea that adopting the internet will allow China to leapfrog to more advanced stages of development has been emphasized by every generation of political leadership in China since the late-1970s. Premier Zhao Ziyang claimed in 1983, for instance, that "the new technological revolution or information revolution… may help China skip over some of the stages which have been experienced by other developing countries" (Taubman, 1998, p. 262). In 2000, Premier Zhu Rongji, once again reiterated in the Fifth Plenum of the CCP Central Committee that "leapfrogging in productivity development may be achieved… by

melding informatization and industrialization, the two processes reinforce each other and progress simultaneously" (People's Daily, 2000).

The country's *Five-Year Plans* – the Chinese Communist Party's guidelines for social and economic development passed through the plenary sessions of the Central Committee and National Congress – have systematically reinforced such instrumental thinking about the internet and its value in nation building. In 1995, the *Ninth Five-Year Plan* formulated the long-term plan for the *State Informationization Plan* and established the goal that by 2010, the internet would constitute the core of the state's information infrastructure. It also emphasized a series of golden projects to modernize the IT infrastructure and support the IT industry. The launch of the *Informationization of the National Economy* (INE) program in 1997 further re-affirmed the application of network technology and its role in improving the nation's productivity and economy performance. The *Tenth Five-Year Plan for National Economic and Social Development* further demonstrated the government's determination to promote the use of internet as part of its aim of informatizing the agricultural sector and pushing forward the e-government project and software industry (People's Daily, 2005). The *State Informationization Strategy* (2006-2020) promulgated in 2005 positioned information and communication technology as a strategic sector (as a "dragon head" industry) and kicked the development of the internet industry into high gear. The *Strategy* further enhanced the internet's role in promoting national economic informatization while adjusting the economic structure and transforming the patterns of economic growth and in building e-government. In March, 2006 the National People's Congress (NPC) reviewed and adopted the Outline of the *Eleventh Five-Year Plan for National Economic and Social*

Development, which envisaged the speeding up of the integration of the networks of telecommunication, radio, television and the Internet, to build the next-generation Internet and accelerate its commercial application (IOSC, 2010).

The instrumental view of the internet is of little surprise given that technological backwardness was one of the reasons for China's historical downfall, especially during the Qing Dynasty. The flip side of the heavy emphasis on the technical potential of the internet is the relative neglect of the social and cultural conditions that underpin the adoption, diffusion and use of the internet. The Chinese government believes strongly that it can strip out the original social cultural meaning of the internet and inject the technology into the Chinese culture. Especially, the goal of Deng's "anti-spiritual civilization campaign" and his successor Jiang Zemin's campaign against all-out Westernization and concomitant "peaceful evolution" followed a familiar pattern of *ti-yong* dichotomy that hark back to late imperial China, with a clear stress on the superiority of Chinese culture and a cautious approach to foreign ideologies (Lagerkvist, 2010, p. 131).

Sovereignty is a reoccurring theme throughout the development of the internet and looms large in the state's rhetoric of internet regulation, and as justification for government censorship. For example, on August 9th 2000, an editorial piece in the Party's newspaper, the *People's Daily*, warned that "enemy forces at home and abroad are sparing no effort to use this battle front [the internet] to infiltrate us" (*People's Daily,* 2000). The article emphasized a fear of cultural imperialism in the age of internet, thus making it necessary to establish and assert national borders on the internet in China. The prevalence of nationalism is so strong and contradictory to the original logic of internet

that some scholars, notably Jack Goldsmith and Tim Wu (2006), claim that: "the government is… grafting Chinese nationalist ideology onto the network itself, in the process literally changing the nature of the Internet in China" (p. 89). In essence, the state has articulated the view that cyberspace will still be bound by national borders and sovereignty. A 2010 government White Paper on the *Internet in China* expresses such views as follows:

> Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected. Citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and conscientiously protect Internet security. (IOSC, 2010)

The Chinese government constantly emphasizes that "cyberspace is not a place outside the legal system"(网络不是法外之地) (People's Daily, 2012). The Minister of Post and Telecommunications Wu Iichuan also stated in June 1995: "Networking does not mean that all information will be allowed to flow in. As a sovereign nation, China must strengthen information management" (Taubman, 1998, p. 264).

4.4 Commercial Logic in the Internet Development

The commercialization and privatization of the media and telecommunication industries was well underway after China's Opening Up and Economic Reform era when the internet was first introduced into the country, circa 1987. In the absence of the familiar state subsidies of the Maoist era, media and cultural units in post-socialist China have ever since been judged by their commercial success in a crowded marketplace (Rosen, 2010, p. 514). Advertising became the single most important non-governmental source of media revenue after it was reintroduced in early 1979 (Zhao, 1998, p. 55). The Chinese media were also encouraged to obtain outside funding through advertising and

increased sales. Although restrictions remain that limit the share of non-state investment in media outlets to 49% or less, the general thrust has been a significant transfer of property from state- to private-ownership (Stockmann & Gallagher, 2011). The bottom line, however, is that economic considerations have driven Chinese communication policies since the reform movement began in 1978 (Kluver, 2005, p. 303).

Historically speaking, the development of telecommunication industries in China has faced a chronic lack of funding and investment (He, 1997). A key reason for this stems from the premium that has been placed on national sovereignty, a focus that has, in turn, strictly limited foreign ownership and investment. Ownership stakes and investment have been especially limited in infrastructure while slightly more accommodating with respect to services (He, 1997, p. 78). For example, Directive No. 54, issued in 1990 by the State Council and a similar circular released by the Ministry of Posts and Telecommunications in 1992, strictly prohibited the operation of joint ventures in the postal and telecommunications sectors (MPT, cited in He, 1997). However, similar to other media reforms, the telecommunications industry was also commercialized and partially privatized. Observing the severe shortage of funding for large projects in many MPT branches, the Ministry issued Directive No. 571 that allowed the branches to set up joint ventures in local and long-distance services, although foreign company's involvment in ownership and managemnt is still banned (Mueller & Tan, 1997, p. 40). Such attempts to balance the needs for investment while retaining state ownership and control over telecommunication has given rise to the argument that the telecommunication sector has become characterized more by market forces and market incentives and less by political purposes (Kluver, 2005). Such commercial motives are

also manifested in the Chinese government's attitude towards the internet as it embraced the economic potentials of internet with open arms: the state intervened in reducing the high cost of internet access and various local governments created their own internet projects in the hope of sharing in some of the economic benefits brought about by the internet. Not only has the state taken a proactive role in promoting and benefiting from the commercial use of the internet, private actors – foreign and domestic – have played an indispensible role in financing network infrastructure and in driving demand for fast communication.

Although the Chinese government invested heavily in building the internet infrastructure (a total of 4.3 trillion Yuan, roughly 691 billion USD from 1997 to 2009) (IOSC, 2010), a lack of investment still prevails as a major problem. The insufficient supply of internet infrastructure has also been a factor behind the high cost of internet access, hindering its wider use in the early stages of its development. Indeed, internet users have identified high prices as a major obstacles to using the internet from early on, as Table 8 below demonstrates. McIntyre's (1997) research on early email usage in China also showed that high cost was a significant roadblock to the further adaption of email in China. For example, in 1991, it cost 8,000 yuan to join ChinaNet and 2,000 yuan per month to maintain services. The charges per kilobyte of information sent or received at the time was 10 yuan whereas the average monthly salary for a professor was 150 yuan (McIntyre, 1997, p.158).

Table 8

Top Three Reasons that Hinders Internet Usage, as Identified by Users

Time	Too expansive	Slow Speed	Not enough Chinese Information
Oct-97	36.2	49.1	7.3
Jul-98	61.2	88.9	45.5
Jan-99	74	92	49
Jul-99	36.8	49.3	9.1
Jul-00	35.7	48.5	6.1
Jan-01	30.8	46.4	6.4

Note. Author's compilation of CNNIC reports, 1997-2001.

Given such high costs, the Chinese government has tried to take a proactive role in lowering price and fostering wider use of the internet since the early days of the internet in the country. Premier Zhu Rongji and other central leaders ordered sweeping cuts in leased line fees and internet access rates in 1999, for example. International leased line fees for Internet Service Provider were cut by 25 percent, from USD $52,000 per month to USD $38,600 per month; internet hourly rates were lowered to roughly USD 48 cents per hour and dial-up rates in Beijing and Shanghai lowered to USD 0.25 cent per minute (Clark, et al,. 1999; Harwit & Clark, 2006). Government intervention not only encouraged the diffusion of the technology but also enhanced the comparative advantage of government-owned organization and secures their monopoly and control over the infrastructure.

Commercial motives and a longing for profit were also clearly manifested in the orientation of many state-owned networks. Different ministries also established their own commercial network infrastructure. For example, China's Educational and Research network (CERNET)'s developers claimed that:

> CERNET has its unique and irreplaceable status among all the Internet competitors in China. We believe CERNET will greatly improve the education and research

> infrastructure in China and train network experts as well as experienced network end users. In a word, it will help to boost China's education, research and economic developments. (Tan, Mueller, & Foster, 1997)

As a result, industrial ministries, national corporations, service organizations and government agencies became the major consumers for internet service as they usually use information systems as a crucial input for their productivity and administration. Local governments in China generally believe that an information and communication network is the prerequisite for local economic growth and expansion (Tan, 1995). Achieving these goals were also coupled with the political goals of enhancing the Party's legitimacy as economic growth helped to lift people's living standards (pp. 304-305).

Besides government organizations, various business enterprises, both domestic and foreign, also played an indispensible role in driving demand for better and faster internet services. Banks, including the Bank of China, were the largest customers of the MPT's CHINAPAC – the largest commercial data network in the country – as well as for other services such as the China International Travel Service (Mueller, Tan, 1997, p. 87). The demand for sophisticated data telecommunications arose from the still-small number of multinational enterprises operating from Beijing, Shanghai, Guangzhou and Shenzhen (Ure, 1997). Large multinational corporations such as the Shell Corporation also maintained their own international computer networks with nodes in China, although the use of such facilities was strictly restricted to company employees (p. 157).

In sum, the internet policy in China has been from its inception an outgrowth of the country's telecommunication regulation, exhibiting many similiarities to the developmental trajectory of the telecommuications industry as a result. In particular, this can be seen in the nationalistic outlook and consistent lack of investment that have

defined telecommunications in China since the late 19th century. At the same time, the internet in China was introduced at a specific historical juncture in the country's industrialization, informatization and economic reform era. This introduced new challenges and opprotunities to the existing regulatory authorities of telecommunication industry.

5 Chapter: Navigating the Market

> Advances in the technology of communications have proved an unambiguous threat to totalitarian regimes: Fax machines enable dissidents to bypass state-controlled print media; direct-dial telephone makes it difficult for a state to control interpersonal voice communication; and satellite broadcasting makes it possible for information-hungry residents of many closed societies to bypass state-controlled television channels – Rupert Murdoch, 1993

> In the new century, liberty will spread by cell phone and cable modem… we know how much the Internet has changed America… imagine how much it could change China… [The Beijing regime] has been trying to crack down on the Internet – Good luck. That's sort of like trying to nail Jell-O to the wall – Bill Clinton, 2000

The optimism about how the internet would democratize China illustrated in the above quotes from Rupert Murdoch and Bill Clinton have clearly failed to mesh with the dynamics of Chinese internet regulation that have taken shape ever since those words were spoken. Given the deep-rooted instrumental thinking towards technology, the government clearly wants to minimize the disruptive social and political impact of the internet while maximizing its commercial benefits. As Jack Goldsmith and Tim Wu (2006) poignantly summarized, China is "trying create an Internet that is free enough to support and maintain the world's fastest growing economy, and yet closed enough to tamp down political threats to its monopoly on power" (p. 89). From the meso-level of the industry, this chapter examines how this dual goal has been enabled and codified at a legal and regulatory level in China: who are the major regulatory authorities that have the power to set the rules of the road that govern private Chinese internet companies? What laws and regulations are in place to regulate the internet business and delegate responsibility for controlling online information flows, while stimulating investment, competition and economic growth? Through a systematic review of published policies

and regulatory documents, this chapter seeks to provide an empirical overview of the legal architecture of internet control in China.

The chapter offers an in-depth look at how private internet companies are regulated in China by examining the key organizations involved in the regulation processes and the laws and informal, voluntaristic methods that are used to regulate internet companies and which require those entities, in turn, to monitor and regulate the activities of their users. Such measures, as will be seen, include state-imposed regulations and administrative measures, industry self-regulation and rules and laws that govern who can and cannot operate within China (e.g. ownership rules, licensing conditions and the general conditions they operate under).

The existing literature on Chinese internet regulation identifies several obstacles that make it difficult to obtain a clear view of the labyrinth of regulations, rules and policies that structure the internet and its operation and control in China. On one hand, the involvement of a large number of government ministries and administrations has resulted in inefficiency and overlapping of responsibilities (Wacker, 2003; Yu, 2012). On the other hand, the clumsy bureaucratic structure of the Chinese government has made control over the internet impractical and comprehensive censorship impossible (Cheung, 2006; Hu, 2011). Heavy regulation of the internet is also coupled with a lack of clearly defined mechanisms for implementing the raft of laws, regulations and rules that have been adopted by various branches of government. Moreover, the law and policy making process in China continues to be characterized by its ambiguity and arbitrariness, and this is only compounded by bureaucratic turf wars as well as competing claims raised by both the central and local governments. As a result, rather than a uniform set of laws,

regulations and rules, such matters are often confusing and vary widely across different websites (Wright, 2013; MacKinnon, 2009). The regulation of the internet is also shaped by different priorities of different generations of political leadership. For example, the third generation of Chinese leadership, as exemplified by President Jiang Zemin and Prime Minister Li Peng, heavily emphasized the technical efficiency of the internet in nation building and economic development. The fourth generation of Chinese leadership, as typified by President Hu Jintao and Prime Minister Wen Jiabao, in contrast, prioritized social stability – the idea of the "Harmonious Socialist Society" as such leaders put it. President Hu, for example, declared: "whether the government can cope with the Internet is a matter that affects the development of socialist culture, the security of information, and the stability of the state" (Lee & Liu, 2012, p. 127).

5.1 Regulators and Regulations

A large number of government organizations and administrative units were engaged in the initial regulation of the internet in China. The inter-ministerial rivalries not only led to a period of relative freedom but also left the legacy of a highly un-coordinated regulatory structure overseeing the internet development in China. This continued to be so even after the bureaucratic re-organization in 1998 that combined the State Council with the Ministry of Posts and Telecommunications, the Ministry of Electronic Industries, and the communication networks of three other government departments – the Ministry of Radio, Film, and Television, China Aerospace Industry Corp, and China Aviation Corp – to create the new 'super agency', the Ministry of Information Industry. As Gudrun Wacker (2003) observes, the result is a tangled mess of regulations and a confusing number of ministries and administrative units (p. 61). To help

clarify the bureaucratic and regulatory landscape, Table 9 below lists the major governmental organizations and administrative units that are involved at the national level in the policy making and supervision of private internet companies in China.

Table 9

Regulatory Organizations of the Internet in China[4]

Organizations	Major responsibility
National Economic Information Joint Committee (1993)	Overall planning
State Council Steering Committee on National Information Structure (SCSCNII) (1996)	Overall planning
Ministry of Information Industry (former Ministry of Post and Telecommunication and Ministry of Electronic Information) (1998)	Network content regulation; Licensing
Ministry of Public Security	Network content regulation, Network Security
The State Administration of Radio, Film and Television (SARFT)	Online Advertising
China Internet Network Information Center	Domain name registration and distribution of IP addresses

Each organization plays different roles, with varying degrees of influence. Each of them also has different responsibilities when it comes to planning and supervision of the day-to-day operation of the internet in China. The Economic Information Joint Committee, established in 1993, but which was later turned into the State Council Steering Committee on National Information Infrastructure (SCSCNII) in 1996, is in charge of overall strategic planning for Chinese Telecommunication and ICT policy. All other ministries, including the Ministry of Information Industry, Ministry of Public Security and the SARFT oversee the day-to-day operations of private internet companies. Although one of the Ministry of Information and Industry's self-declared mandates is to

[4] Here I have only listed the regulatory bodies that play an important role in overseeing the private internet companies in China. Some other organizations, such as the Ministry of Commerce, are also involved but because these organizations often do not play a crucial role in policy-making and in overseeing day-to-day operation. They are omitted from the chart in this thesis.

"formulate strategy, policy and plans for the information, telecommunication and software industries", it also supervises the telecommunications and information services market and the licensing process (MII, cited in Cullen and Choy, 1999). The Ministry of Public Security, on the other hand, is mainly responsible for monitoring and controlling internet access and use – steps that, crucially, include keeping the registration records of internet users and investigating and prosecuting crimes committed online.

As indicated above, internet companies in China are subject to regulations enacted and overseen by both the national and local governments. As Henry Lu (2011) states, commercial networks not only have to comply with local telecom regulatory agencies' requests to self-censor, they also need to accept supervision from local branches of the Ministry of Industry and Information. Sometimes this leads to conflicts between the central and local governments and to the inconsistent application of internet censorship. As noted by Jonathan Lagerkvist (2010), the delegation of control to commercial internet businesses and reliance on lower-level bureaucrats always brings a risk to the Party. The leaks of blacklists of keywords that commercial Internet businesses must follow to accommodate Party-state pressure is an example. The delegation of control to commercial internet business, therefore, creates many give-and-take processes between propaganda officials and actors in the state-controlled media system, as noted by Lagerkvist (2010, p. 148).

Table 10 below lists major regulations that are applicable to private internet businesses in China at the national level. Viewed in a chronological order, internet regulation in China grows more comprehensive, intensive and engages a wide range of state and non-state actors. In the late 80s' to early 90s' when the internet started to

develop in China, there was less intensive and systematic regulations on private internet enterprises operating in China. Ownership rules promulgated by the Ministry of Posts and Telecommunications during this period, for instance, restricted foreign companies to operate and own telecommunication infrastructures.

Table 10

List of State Regulations on Private Internet Enterprises

Year	Name	Organization
1994	Rules of Security Protection of Computer Information Systems	State Council
1994	Regulations For Safety Protection of Computer Information Systems	State Council
1996	Interim Regulation on Administration of International Networking of Computer Information Networks	State Council
1997	Computer Information Network and Internet Security, Protection and Management Regulations	Ministry of Public Security
2000	Administrative Provisions for Electronic Bulletin Services on the Internet	Ministry of Information Industry
2000	Administrative Measures on Internet Information Services	State Council
2000	Decision of the National People's Congress Standing Committee on Guarding Internet Security	National People's Congress Standing Committee
2000	Regulations on Telecommunications of the People's Republic of China	State Council
2000	Administration of Engagement by Internet Sites in the Business of News Publication Tentative Provisions	Ministry of Information Industry
2001	Provisions on the Administration of Foreign-funded Telecommunications Enterprises	State Council
2002	Regulations on Administration of Business Premises for Internet Access Services	State Council
2006	Regulations on the Protection of the Right to Network Dissemination of Information Networks	State Council
2012	Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks	National People's Congress Standing Committee

It was not until 1994 that the legal foundation giving the government the authority to control and monitor computer networks was established through the *Rules of Security Protection of Computer Information Systems* (Sohmen, 2001, p. 19; Taubman, 1998, p. 264). Comprising 17 articles, the *Rules of Security Protection of Computer Information Systems* is the prototype for current internet regulation in China. The *Rules* stipulate that the establishment of international links has to be approved by the Ministry of Posts and Telecommunications (Article 6). The *Rules* ban any internet business that endangers national security, leaks state secrets, threatens social order or distributes pornographic information (Article 13).

1996 marked a key year when the Chinese government clamped down on the internet. The government established the legal foundation that delegates the responsibility to control online information flows to private internet companies, which is comprised of three sets of rules (Cheung, 2006; Mueller & Tan, 1996). The first formal and comprehensive set of rules were stipulated in 1996 by the State Council: the *Interim Regulation on Administration of International Networking of Computer Information Networks*. The regulation was revised and incorporated in 1997's *Computer Information Network and Internet Security, Protection and Management Regulations* by the Ministry of Public Security. Articles 6 and 7 of the *Interim Regulations* required all networks with international connections to register with one of the following state-authorized organizations: Ministry of Post and Telecommunication (MPT), the Ministry of Electronics Industry (MEI), the State Education Commission (SEC), or the Chinese Academy of Sciences (CAS). The government also required all internet users to register with the local police within 30 days from the day the regulation took effect (PRC, 1997).

Shortly thereafter, the Ministry of Post and Telecommunication temporarily shut down ChinaNet in Beijing and Shanghai in order to install software to filter antigovernment and pornographic websites from overseas (Reuters, cited in Mueller & Tan, 1996, p. 92).

On the eve of China's accession to the WTO, another raft of internet regulations was promulgated. In one year alone (2000), six major internet content control regulations were promulgated by the National People's Congress, the State Council, and the Ministry of Information. Legal scholar Anne Cheung (2006) argues the delegation of policing power to non-state actors was the centerpiece of this raft of legislation, and similar measures that have been adopted ever since (p. 11). Other observers argue that these efforts sought to hastily put into place a series of strong internet controls *before* China's accession to the WTO in 2001 (Cheung, 2006; Weber & Jia, 2007; Wacker, 2003).

These regulations form the basis of the legal architecture of internet regulation in China. They cover three broad categories: content regulation, intermediary liability and market access and behaviour rules (ownership and licensing rules). Together with the Internet Society of China's self-regulation rules, they form the legal and regulatory framework that all internet companies must obey when operating in the Chinese marketplace. The following section analyzes the rules that fit under these categories in greater detail.

5.2 Market Regulations

5.2.1 Ownership Rules

In order to operate in the Chinese market, private internet companies have to abide by the series of regulations briefly outlined above. This remains the case despite the fact that China became a member of the World Trade Organization in 2001. Although

China relaxed its foreign ownership rules on its accession to the WTO, a lengthy list of restrictions was set out in the *Administration of Foreign-funded Telecommunications Enterprises Provision* adopted in 2001 at the same time that China was joining the WTO. Under these rules, foreign companies must enter a joint venture with domestic partners to enter the domestic market. Article 6 of the *Provisions* also limits foreign-ownership in telecommunications enterprises to 49%, while foreign investment is allowed to take up to 50% of ownership in value-added telecommunications services.

5.2.2 Licensing Requirements

Operators of telecommunication businesses are also required to obtain operating permits by the supervisory department for the information industry under the State Council or the local telecommunication administration authorities (Article 7 in the *Administration of Foreign-funded Telecommunications Enterprises Provision*, as well as Article 7 in the *Telecommunications Regulations of the People's Republic of China*). These licensing rules are also mandatory for any internet companies that seek to operate in China.

Different types of internet services are subject to different ministries' licensing requirements. For example, Internet Content Providers (ICPs) have to register with the Ministry of Industry and Information Technology; Internet Access Providers have to register with the Ministry of Culture and online news services have to obtain a license from the Press Office of the State Council. The operating permit number or filing number have to be displayed on the homepage of each website.

5.2.3 Industry Self-Regulation

The Internet Society of China (ISOC) has developed and oversees a set of self-regulatory measures that all of its members must follow. With the mission to "formulate self-regulation of the internet industry and bring self-regulation of the internet into full play", the ISOC includes many national research institutions (e.g. the Chinese Academy of Science), as well as Chinese telecoms and internet giants such as China Unicom, Sina Corporation, Huawei Technologies Co., Ltd and Baidu. In 2001, the ISOC published the *Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry*. The stated reason for this approach was to achieve greater transparency in the to self-regulatory practices followed by internet companies in China and to promote the commercial use of the internet, especially after China joined the World Trade Organization. Ian Weber and Lu Jia (2007) argue that such efforts, although perhaps seeming to be fairly benign at first blush given their emphasis on promoting internet use, preventing cyber crimes and fostering competition, reveal a number of restrictions that hinder the free flow of information and civic engagement (Weber & Jia, Internet and self-regulation in China: the cultural logic of controlled commodification, 2007).

In particular, the content regulations that are the centerpiece of the code stand out as being particularly problematic. For example, Article 9 of the Pledge states:

> We internet information service providers pledge to abide by the state regulations on internet information service management conscientiously and shall fulfill the following disciplinary obligations in respect of Internet information service: 1. Refrain from producing, posting or disseminating pernicious information that may jeopardize state security, disrupt social stability, contravene laws and regulation and spread superstition and obscenity. (ISOC, 2002)

5.2.4 Content regulation

One of the most important elements of Chinese internet regulation is content regulation. As the OpenNet Initiative (2010) makes clear, "underlying all regulation of the Internet is a pantheon of proscribed content" (p. 456). This is especially true of China where the government has created nine broad categories of "illegal content" through a labyrinth of laws. The long and troublesome list of forbidden content includes:

> (1) content that violates the basic principles of the Constitution;
> (2) content that impairs national security, divulges state secrets, subverts state sovereignty, or jeopardizes national unity;
> (3) content that damages the reputation and interests of the state;
> (4) content that incites racial hostilities and ethnic discrimination or jeopardizes unity among the ethnic groups;
> (5) content that damages state religious policies or that advocates cults or feudal superstitions;
> (6) content that disseminates rumors, disturbs the social order, or damages social stability;
> (7) content that disseminates obscenity, pornography, gambling, violence, homicide, or terror, or incites crime;
> (8) content that insults or slanders others or that infringes on others' legal rights and interests;
> (9) other content that is prohibited by laws or administrative regulations.

These categories are vaguely and ambiguously defined and cover a wide range of content. They are scattered throughout a tangled web of laws and bureaucratic procedures, as the long list that follows illustrates so well: *Computer Information Network and Internet Security, Protection and Management Regulations* (1997), *Administrative Measures on Internet Information Services* (2000), *Regulations on Administration of Business Premises for Internet Access Services* (2000), *National People's Congress Standing Committee Decision Concerning Safeguarding Internet Safety* (2000) and *Administrative Provisions for Electronic Bulletin Services on the Internet* (2000). All of these seemingly distinct pieces of legislation lay out the same categories of forbidden content.

Many scholars have argued that the vague and ambiguous wording used to identify so-called forbidden content is intentional. Such ambiguities counter the veneer that the 'rule of law' holds sway in China with the reality that there is basically an unbounded space for the government's own interpretations of what constitutes 'illegal content' to prevail. Such ambiguities also encourage widespread self-censorship among citizens who have no idea as to where the real boundaries of what is legal and illegal lay. A constant fear of offending the ruling regime prevails as a result (Cheung, 2006; Wacker, 2003, p. 69; Taubman, 1998; Sohmen, 2001).

The legal regime also carves out an equally nebulous terrain upon which internet intermediaries are obligated to function as agents on behalf of the state. Article 16 of the *Administrative Measures on Internet Information Services,* for instance, requires internet service providers to report to relevant state authorities when information transmitted on their websites falls into any of the above mentioned prohibited categories. In cases where an internet business fails to report such matters, the government can hold them liable and punish them, including, in more serious cases, by removing their business license and ordering their service, website, etc. to be shut down (Article 23). These latter measures in particular constitute a strong effort by the government to offload censorship responsibilities on to private internet companies. In effect, the government has made private, commercial companies responsible for policing content on their networks and websites, effectively turning them into handmaidens of state internet controls. Of course, the rigid yet ambiguous regime of content regulation is just as often as not inconsistently enforced, as Rebecca MacKinnon demonstrated by testing the accessibility of a variety of censored words across different blog websites in 2009. Nonetheless, the Chinese

government's approach to content regulation places enormous pressure on internet companies to self-censor content that might jeopardize their business.

It is worth mentioning that delegating the responsibility to closely monitor and control information is not new. In fact, telegraph companies were required to police messages sent across the wire long before the internet was even a conceptual idea. As Article 28 in the *Provisional Regulations on Domestic Telegraph Operation* (1949) stated: "if the telegraph service station, based on fact, judges that the content of a telegram is harmful to the national or people's interest, the matter should be handed over to the local government" (Zhou, 2006, p. 132). In other words, internet regulation in China is a piece of the country's long-standing approach to telecommunications regulation more generally. As a result, regulation that is already in place can sometimes be grafted on to the regulation of new technologies such as the internet.

5.2.5 Collection and Storage of User Data

Article 14 of the *Administrative Measures on Internet Information Services* stipulates that for information service providers engaged in news, publishing and electronic notice services shall record the content of information distributed and the time distributed, as well as internet addresses and domain names from which such information originated. Even stricter data retention requirements are imposed on internet access providers. They are required to record "user online time, user account numbers, Internet addresses or domain names and the principal telephone numbers of internet users" (ChinaITLaw, 2010). The collection of users' personal identification number is further re-enforced in Article 16 of the *Regulations on Administration of Business Premises for Internet Access Services*:

> A unit operating business premises for Internet access services shall check and register the identity cards or other valid credentials of consumers of Internet access services, and make a record of relevant log-on information. The registered contents and copies of the record shall be kept for a period not less than 60 days, and shall be provided to the culture administration department and the public security organ when they conduct an inquiry according to law.

The extensive data collection process engages both physical data, such as the address, phone number and national identification card number, as well as digital footprint of internet users such as log times and account numbers. Furthermore, internet companies are required to keep user data for a period of 60 days and to disclose it under ambiguous terms, i.e. when an inquiry by either public security or cultural administrative agencies is being conducted as opposed to, for example, a court order, warrant, etc.

5.2.6 Penalty

Article 23 of *Administrative Measures on Internet Information Services* establishes several penalties that can be meted out when internet companies fail to report content that violates the aforementioned nine forbidden categories. The penalty for non-compliance will result in a range of consequences, ranging from RMB 5,000-50,000 for not showing a business license number on the website to the revocation of a business license if the website fails to delete content that violates any of the nine forbidden categories. By putting internet companies in charge of policing content on their networks and websites, the strict penalties imposed by the government create a legal and normative environment that encourages internet companies to self censor, and to do so broadly rather than in a narrowly targeted and precise way.

5.2.7 Intermediary liability

While the government has set into place a sprawling approach to content regulation, it has also struggled to avoid inhibiting the commercial potential of the

internet. Anne Cheung (2006) characterizes the dilemma as follows: "the major challenge for the Chinese Communist Party is to attain the optimal level of information flow that is conducive to business transactions while preventing unfettered political or social discussion that could disrupt social stability and threaten state security" (p. 2). One offshoot of this general condition, aside from the strict content regulation, is that the state has created a regulatory regime that minimizes the liability of internet companies in case of copyright infringement to keep up with the Western standard and to stimulate investment.

The Safe Harbor provision that limits internet companies' liability with respect to copyright once certain steps have been taken was first established in the Digital Millennium Copyright Act in the U.S. in 1998. Its purpose is to encourage Internet Service Providers to respond to copyright complaints with content takedowns for which they gain immunity from liability for copyright infringement. The cost, however, is that internet intermediaries take on the role of policing content on behalf of copyright claimants while diminishing the rights of their subscribers and users (Seltzer, 2010). Such Safe Harbor measures provide online service providers immunity from damages on the grounds that intermediaries do not themselves host content but are merely conduits for it. In other words, it is a case of 'don't shoot the messenger' (Zittrain, p.14). Ultimately, the Safe Harbor rule aims to stimulate investment and create a regulatory environment that is conducive to business transactions by setting out the conditions under which internet companies must monitor and address content-related complaints in return for protecting them from civil and criminal liabilities.

Emulating the Safe Harbor rule devised in the U.S., three regulations were put into effect in early 2000 that limited liability for internet businesses: the *Administration of Internet Information and Service Procedures*, the *Administration of Engagement by Internet Sites in the Business of News Publication – Tentative Provisions*, and the *Administrative Provisions for Electronic Bulletin Services on the Internet*. In 2006, the promulgation of *Regulations on the Protection of the Right to Network Dissemination of Information Networks* further limited the liability of internet intermediaries in case of copyright and intellectual property infringement. These three regulations provide protection to online service providers in the case of copyright infringement and therefore limit the legal risks these companies may face, similar to conditions in the United States and the European Union, where similar measures have been adopted.

In sum, the Chinese government has built a stringent legal and regulatory architecture that eventually delegates the responsibilities to police online content and user activities to private internet companies by imposing harsh punishment like economic sanctions or suspension of business license. However, by adopting rules like the Safe Harbor provision, this stringent legal architecture also stimulates investment and economic growth. Weibo, China's biggest microblogging service, offers a good example of how one private internet company in China manage to fulfill the government's quest to police online content while also succeed in meeting the goal of maximizing profits for its shareholders.

6 Chapter: The Case of Weibo[5]

This chapter uses Sina Weibo, one of China's most popular and active microblog websites, as a case study to examine how a commercial Online Service Provider (OSP) manages the state's appetite to closely monitor online information flow while also striving to mitigate the negative impact of political controls on its profitability. This case study aims to shed light not just on Weibo but other commercial internet enterprises that share similar conditions on account of their operations in the Chinese market, such as Renren and Tencent, both of which are publicly-listed companies on the NASDAQ and the Hong Kong Stock Exchange. The analysis also aims to provide an empirical account of end users' experience of Weibo with regards to how control is exerted in the technical design of the website, in its legally-binding, click-through user agreement and through various rules that discipline the online community. In particular, this chapter seeks to answer the following question: how does Weibo encourage user participation, which will help generate greater commercial profit and web traffic, while simultaneously fulfilling the government's quest to monitor online content?

This chapter begins by looking at the company that owns Weibo – Sina Corporation, its ownership structure and business model. As a publicly traded company on NASDAQ, Sina Corporation is required by the U.S Securities and Exchange Commission to file its corporate Annual Report and other financial reporting documents. The audited yearly report offers good insights into the operation and business model of the company. Through a critical examination of Sina's Annual Report, this chapter will look at how the state-imposed regulations analyzed in Chapter 4 have an impact on the

[5] When Sina Weibo launched its Initial Public Offering in April, 2014, it changed its name from Sina Weibo to Weibo.

operation of Weibo. I will then go on to critically examine how, as an Online Service Provider, Weibo integrates its responsibility to control web content into the terms and conditions set for user participation, including *Sina Terms of Service*, *Weibo Terms of Service*, *Weibo Community Rules*, *Personal Information Rules* and Weibo user verification system. Other than the terms and conditions set by Weibo, I will examine two recent state regulations that govern the condition of online participation for Weibo – one that establishes a real name policy for Weibo users and another that tackles online rumors. Last but not least, this chapter will analyze the tension between the commercial imperative of Weibo and its responsibility to police internet content and user expression using an example of the User Credit Score system implemented in 2012.

6.1 Sina Corporation

Sina Corporation was formed in 1999 when Stone Rich Sight Information Technology Ltd – a company established by former Sina CEO Wang Zhidong – merged with the United States-based website company, Sinanet.com. Sina Corporation had its Initial Public Offering on the NASDAQ in April 2000. Today it is the world's 14th and China's 4th most visited website (Alexa.com, 2014). Table 11 shows the revenue of top publicly traded internet companies in China, with Sina ranked as the fifth largest company by revenue in the Chinese market[6]. Sina Corporation has seen its revenue grow massively from $942,000 USD in 1996 to $529 million USD in 2012 (see Figure 2). Advertising is Sina Corporation's primary source of income. As shown in Figure 3, other than the years 1999, 2003, 2004 and 2005, advertising revenue has consistently constituted over half of the company's annual revenue.

[6] Sina ranks the sixth if Alibaba, a Chinese e-commerce company, is added to the list. Alibaba is the biggest internet company in China but it is not a publicly traded company therefore it is not listed in the table.

Table 11

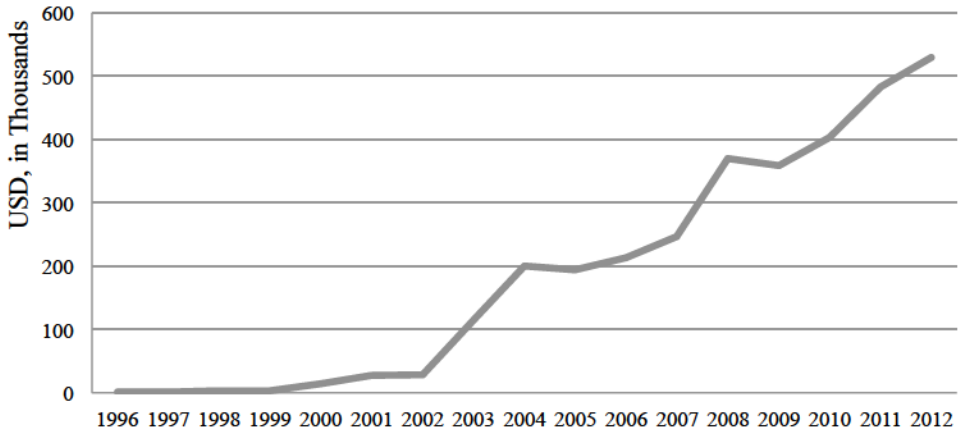
Revenues of China's Publicly-Traded Internet Companies

Company	2009	2010	2011	2012	2013
Tencent	2006.5	3168.7	4596.1	7079.7	9747.9
Baidu	717.4	1276.6	2338.8	3597.7	5276.8
NetEase	616.7	912.9	1205.3	1351.6	1519.1
Sohu	N/A	612.8	852.1	1067.2	N/A
Sina	358.6	402.6	482.8	529.3	665.1
Renren	N/A	N/A	111.5	159.6	156.7
Sina Weibo				**65.9**	**188.3**

Note. Corporate Annual Reports.

Figure 2

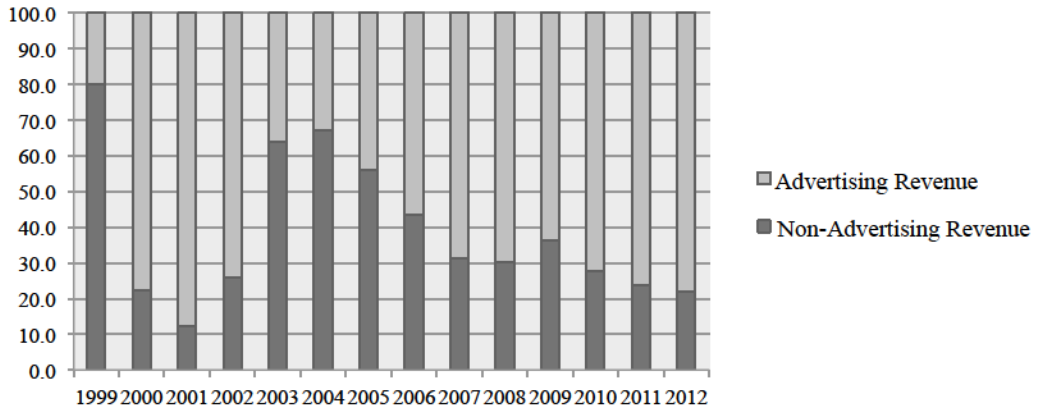
Total Revenue Growth for Sina Corporation, 1996-2012



Note. Sina Corporation Annual Report, 2000-2013.

Figure 3

Sina's Advertising Revenue vs. Non-Advertising Revenue



Note. Sina Corporation Annual Report, 2000-2013

Table 12 shows the ownership structure of Sina Corporation. Sina Corporation is owned by multiple stakeholders with no single party owning a significant portion of the company.

Table 12

The Ownership Structure of Sina Corporation

BlackRock, Inc	8.30%
Thornburg Investment Management	7.00%
Platinum Investment Management Ltm	6.40%
T Rowe Price Associates, Inc	5.60%
Charles Chao	2.00%
All directors and executive officers as a group	2.80%

Note. Sina Annual Report, 2013

The ownership structure of Sina Corporation exemplifies a general tendency when it comes to modern corporations, namely that capitalists are gradually ceding control and power to a professional and technical class of workers. Gradually, there is a divorce between ownership and management with a different social group or class – the managers

– becoming the dominant class (Demers & Merskin, 2000). This is due to the enormous capital requirements of large corporations and increasing complexity of technologies. Under such conditions, company owners have to depend on knowledge workers and professionals to run the new means of production. Based on the ownership structure, Sina is not an owner-controlled company. However, Charles Chao, who is also the Chairman of the company's Board of Directors and Chief Executive Officer, owns 2 percent of Sina Corporation.

6.2 Why Weibo?

Launched in August 2009, Weibo is a microblogging service offered by Sina Corporation. Bearing much resemblance to Twitter (e.g. both allow only 140 characters in every post), Weibo is often regarded as its Chinese counterpart. Within five years of its operation, Weibo quickly gained popularity among its competitors such as Tencent Weibo and Fanfou. As a spin off from the Sina Corporation, Weibo launched its Initial Public Offering in April 2014, its revenue ($188.3 million USD) ranked close to that of Renren (156.7 million USD) in 2013, the fifth largest publicly-traded internet company in terms of revenue in China. Weibo is now owned by Sina (58%) and Ali WB Investment Holding Ltd, a wholly owned subsidiary of Alibaba, a Chinese e-commerce company (Weibo, p. 39).

With a rapid increase in its user population (from 10 million in 2010 to over 600 million in 2014), the popularization of Weibo has incited a wave of optimism about the democratizing potential of such Twitter-like media platform, especially given its role in spreading news about events such as the 2011 Wenzhou province high-speed train crush and Sichuan earthquake. The *Washington Post* named Weibo a "free-speech platform"

because of its role in facilitating communication amongst citizens during these events and praised its power in shaping public opinion and its potential for social organizing (Richburg, 2011). Many recent scholarly studies (Huang & Sun, 2014; Tong & Zuo, 2014) also recognize Weibo's instrumental role in the development and dissemination of collective action and social movements both online and offline, arguing that Weibo is a "breeding ground for mobilization" (Huang & Sun, 2014, p. 98). Others, however, argue that Weibo provides the government with an opportunity to benefit from popular knowledge about local disputes and protests. Furthermore, by helping to spread the news about its punishment of local officials, Weibo helps to enhance the government's legitimacy (Tong & Zuo, 2014).

Scholars like John Sullivan (2013), in contrast, argue that claims about the democratic potential of Sina Weibo ought to be treated with caution because as microblog users increasingly vent their discontent with various social ills online, the government is also growing more adept at harnessing information online to identify and neutralize threatening behavior. Moreover, with the promulgation of the Real Name Registration policy in 2012 in tandem with the government's campaign to curb the dissemination of online rumors in 2013 and 2014, the initial optimism circulated in the mainstream media about the democratizing potential of microblogs has slowly died down. Concerns have also been raised about the recent decrease in Weibo's user population, the extent of their activity, and the company's profit outlook, especially when compared to rival Tencent's WeChat (Custer, 2014; Yilun, 2014; Millward, 2013).

Nonetheless, the impact of Sina Weibo on the Chinese society cannot be under-estimated. For example, *People's Daily* named year 2010 "Year One of the Microblog"

(微博元年) and 2011 "Year One of the Government Microblog" (政务微博元年) to acknowledge the mass popularity of Weibo and its wide adoption rate among various government officials and organizations. Indeed, as evidence of the latter and as of 2011, there were nearly 20,000 registered government official accounts on Sina Weibo (*People's Daily*, 2011).

6.3 Weibo Regulated

With more than 600 million registered users (Sina, 2013), Weibo provides a venue for internet users from all walks of life to interact with each other: average users, commercial entities, and increasingly, many government officials and organizations have signed up for a Weibo account. This section examines how Sina Weibo mobilizes different mechanisms to secure political control over network content while simultaneously encouraging user activity and interaction. From an end user's point of view, this chapter looks at how Weibo integrates elements of self-censorship into both its user contracts and technical design.

6.3.1 Conditions of Participation

Upon signing up for an account, all Sina Weibo users have to abide by five important regulations: *Sina Terms of Service*, *Weibo Community Guidelines*, *Weibo Terms of Service*, *Weibo Personal Information Protection Policy* and *Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks*. These five contracts outline the basis of service provision and condition of participation. The requirement that users obey these regulations is indicated on both the sign-up page and in the column on the right hand side of each individual

user's Weibo homepage. Such prominent visual cues constantly remind users that their activities on Weibo are tightly governed by a distinct set of rules (See Figure 4).

Figure 4

An Example of Weibo User Page

Laura Stein (2013) argues that, while often ignored, these "click-through" contracts set the condition of participation on the internet and also act as legal agreements that users can rely on in the event of conflicts. In particular, these five user contracts list the terms and condition for the collection, disclosure and retention of user data and company liability with respect to users activities. These aspects are crucial to this thesis because they help to illustrate the roles and responsibilities of Online Service Provider.

Article 5 of *Sina Term of Service* and Rule of Use 4.1 of *Weibo Term of Service* require users to register with "accurate personal information". In other words, users are required to subscribe to the service using their real names rather than either anonymously or by using a pseudonym. Users' information will be disclosed under two circumstances, the *Terms of Service* indicate: for the protection of public interests or according to the relevant laws, regulations and government authorities that govern Weibo's operations

(see section 6.2 in *Weibo Term of Service* and Section 7 in *Sina Term of Service*). In case of copyright infringement, Sina's policy is consistent with what is listed in the *Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks*, where the online service provider assumes limited liability in case of copyright infringement. As section 6.1 of Sina *Terms of Service* stipulates:

> Sina company will not be responsible to the users or any third party in any form regarding any delay, inaccuracies, errors and omissions or any damages arising or caused during the transmission or submission of all part of the copyrighted content. (Sina, 2012)

Given that Weibo also provides services to many overseas users, Section 11.2 of *Weibo Term of Service* specifies that the legal jurisdiction is in China: "the formulation, implementation and interpretation of this Agreement, as well as the dispute settlement are subject to Chinese law and under the jurisdiction of the courts of China" (Sina, 2010). Most notably, in case of users posting content that violates existing laws and regulations, the *Weibo Terms of Service* indicate that the company will closely monitor user activity and delete user posts, without notification, whenever the company believes that doing so is necessary to fulfilling its obligations under Chinese law and in line with its business interests. Section 4.9 of the *Terms of Service* states these points as follows:

> Weimeng Company reserves the right to review and monitor the user's Weibo service use situations (including but not limited to audit the contents stored on Weibo platform by the users). If a user violates any of the above requirements while using the Weibo Services, Weimeng company or its authorized entities have the right to require the user to make corrections or to take all necessary measures directly (including but not limited to, change, or delete the contents posted by the user, suspend or terminate users' right to use Weibo service), so as to eliminate or mitigate the impact of user's misconduct. Prior to, during and after the aforementioned operations are completed, Sina does not need to notify the users in any way (author's translation).

Section 4.9 in *Weibo Terms of Service* enables company surveillance and censorship. For example, when a post is deleted by Weibo, the company usually does so without notifying the user but the censored post will be replaced with the message that: "sorry, this post isn't suitable for the public. If assistance is needed, please contact customer service" (author's translation). In some instances, the web administrator will "encrypt" the censored post to make it invisible to the public and in this case, users are not responsible for the content posted. Figure 5 is an example of this point derived from an experiment in which I posted a Weibo message that contains censored information. The system administrator "encrypted" my post and sent me a message afterward, stating: "sorry, your post has been encrypted. This post isn't suitable for publication. If assistance is needed, please contact customer service [link to Weibo customer service]" (author's translation).

Figure 5

Notification of a Censored Weibo Post

In addition to the conditions listed in the company's *Terms of Service*, two other regulations were promulgated by the state in 2011 and 2012 further limiting Weibo users' freedom of expression.

6.3.2 A "Real" Weibo

In December 2011, the Beijing Municipality, together with Beijing Public Security Bureau and Beijing Internet Information Office issued new regulations requiring that Sina and other microblog hosting companies implement a Real Name Registration system as of March 16, 2012. The basic effect of the *Beijing Municipal Provisions on Microblog Development and Management* was to outlaw "false microblog users", or in other words, to ban the use of pseudonyms and anonymity online. The intention of the measures is to discipline Weibo users and to establish a healthy and safe online environment, according to the *People's Daily* (2011). As a result, the new regulation mandates microblog service like Weibo to register every new user with their real identity (such as phone number or national ID numbers) while still allowing them to adopt a different screen name. Later in December 2012, this Real Name Registration rule was formalized and made national in scope in the *Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks*.

Weibo facilitated the aims of the new legislation by putting a user verification system in place to actively encourage individuals to verify their identity. In order to become a verified user on Weibo, one has to provide a clear profile picture, link their cellphone account with their Weibo account, obtain a minimum of 100 followers and befriend two other verified users. Once the account passed the verification process, the word "V" will appear besides the user names. On the most influential Weibo account list

(ranked by numbers of followers), all accounts are verified users. Weibo creates hurdles for unverified users in the comment functions. For example, the message in Figure 6 below is an example that a verified user can limit the comment function to users who have linked their cellphone account with their Weibo account.

Figure 6

Weibo Comment Restricted for Unverified User

Weibo's user verification system works hand-in-hand with the Real Name Registration policy to encourage users to register with their real identity by limiting certain commonplace uses of the service only to those who have a verified account on Weibo. These rules are problematic because instead of anonymity, they encourage the norm of identifiability in online participation. These two mechanisms increase user's traceability and with collected personal information and cellphone accounts, the company obtains a greater ability to retain and disclose subscriber information, both for commercial purposes and in line with government demands. The tradeoff for Weibo users is that getting a verified account allows them to do more of the activities possible on the service but at the cost of having to reveal a great deal of more personally identifiable information to Sina, thereby making themselves easier to monitor, control and discipline.

6.3.3 Moral Appeals and the "Seven Baselines"

On March 20th, 2012, rumors about a coup in Beijing organized by allies of Bo Xilai were disseminated widely on Weibo. Chinese authorities shut down sixteen websites and detained six people responsible for "fabricating and disseminating online

rumors" as a result (Xinhua News Agency, 2012). Weibo itself was punished by the State Internet Information Office and forced to shut down the comment function of its service for three days from March 31st to April 2nd (Sina, 2012). This temporary suspension of one of Weibo's most important functions prefaced a new wave of clamping down on online rumors and defamations.

In August 2013, the State Internet Information Office, a department under the State Council that directs, coordinates and supervises online content (Xinhua, 2011), the Internet Society of China, and the Beijing Network Industry Association hosted the *Online Celebrity Social Responsibility Forum*. This Forum was broadcast live on the China Central Television Station (CCTV) during a prime time talk show. Fourteen Big "V" Weibo users (verified users with more than one million followers) were invited. Following the televised discussion, the "Seven Baselines" were adopted as guidelines for online conduct by the *Chinese Internet Conference*, an event hosted by the Internet Society of China in September 2013 (Xinhua, 2013). The *Nanfang Daily* (2013) stated that greater social responsibility and "cleansing the online environment… requires internet users' self-discipline and self-censorship… while rejecting online rumors and spreading positive energy". The Seven Baselines adopted at this time are not formal regulatory measures but more of a call for self-regulation among internet users, especially among Weibo celebrities who are most vocal in online discussions.

These Seven Baselines call on Weibo users to help maintain:

1. Laws and Regulations
2. Socialist System
3. National Interest
4. Citizens' Rights and Interest
5. Public Order
6. Morality

7. Information Accuracy (Bandurski, China's "seven base lines" for a cleaner internet, 2013)

Although the Seven Baselines aim to discipline average internet users, it's real intention was to manage the wide impact that Weibo celebrities have – a big concern for the Party. On August 26, 2013, an editorial in the *People's Daily* stated that the "big Vs" have become an amplifier of "big rumors", given that their accounts are followed by millions of users and re-tweeted by millions (People's Daily, 2013). Within a short period after the guidelines were adopted, Weibo suspended 3773 accounts for running afoul of the Seven Base Lines out of a total of 103,673 accounts punished for a range of 'offenses' (People's Daily, 2013).

The formulation of the Seven Baselines marked the start of a full-fledged government crackdown on online rumors. A month later, a new legal "interpretation" was set out by the Supreme People's Court and the Supreme People's Procuratorate on September 10, 2013 that made it possible for the government to rely on provisions in Article 246 of China's *Criminal Law* to deter and punish online critics (Lubman, 2013). The interpretation expanded the reach of Article 246's definition of criminal defamation to specifically include online content. According to Article 246, disseminating defamatory information through networks, especially when the posted content is reviewed over 5,000 times, received 5,000 clicks, or was reposted over 500 times constitutes a criminal offence (*People's Daily*, 2013). Moreover, the interpretation also further expanded the criminal offense of "endangering social order and national interests" to include network content that contributes to: 1) group mobilization 2) public chaos 3) conflicts between ethnic and religious groups 4) defaming multiple individuals and having a negative impact on society 6) endangering the national image and national

interests 7) and have a negative international impact (author's translation) (*People's Daily*, 2013). A 16-year-old boy, Yang Zhong, who publicly questioned investigators over the mysterious death of a karaoke club manager in Gansu Province on Weibo become the first victim after the promulgation of the new interpretation of the *Criminal Law*. He was accused of spreading online rumors with a Weibo post that was re-tweeted over 500 times and sentenced to three years in jail but was soon released by Public Security authority under public pressure (Jacob, 2013).

The *Seven Baselines* represents a soft version of self-censorship. The call for responsible online conduct behind these guidelines is representative of the Chinese government's moral rhetoric in justifying control on the internet. As Jonathan Lagerkvist (2010) argues, the evolution of delegated self-censorship to online media organizations is reinforced by conveying notions of "healthy content", "harmful information", and burdening journalists and editors with the request to contribute to the construction of a "harmonious society" (p. 143). Furthermore, the combined effect of the *Seven Baselines* and the new interpretation of the *Criminal Law* represents an evolution in the means of internet control: from blocking, filtering and denying access through control over the technical and physical infrastructure of the internet to the creation of a legal and normative environment that enables the Chinese government to deny access to information resources as and when needed, while reducing the possibility of blowback or discovery. These are all constitutive parts of what the OpenNet Initiative has called "second generation of internet control" (Deibert, Rohozinski, Palfrey, et al., 2010, p. 24). The promulgation of these new regulations on online rumors and defamation carves out an environment that encourages user self-censorship, especially among those who have

many followers on Weibo. The expansion and application of the new definition of criminal offense into the online context – with its nebulous conception of social ills to be avoided – also further establishes a questionable legal base, which the state has used to tighten its censorship online. These two new legal regulations imposed on Weibo represent the second generation of internet control, where "the overt track aims to legalize content controls by specifying the conditions under which they can be denied" and by using instruments like the doctrine of information security and existing laws, such as slander and defamation, to squelch objectionable speech online (Deibert et al., 2010, p. 7).

6.4 A Delicate Balance Between Profit and Politics

As a public-traded, privately owned company, Weibo is not only subject to state regulations that are listed in the State Council's *Administrative Measures on Internet Information Services*, *Regulations on the Protection of the Right to Network Dissemination of Information Networks*. It must also abide by various regulatory directives issued by local governments. These measures, all of which aim to control and direct online content, also collide with the company's imperative to maximize profit. Concerns about the impact of the Chinese government's heavy-handed approach to internet content regulation on the profitability of Weibo are constantly highlighted in the company's annual reports:

> … government regulation and censorship of information disseminated over the Internet in China may adversely affect our ability to operate Weibo… the PRC government may prevent us from advertising or distributing content that it believes is inappropriate and we may be liable for such content or we may have to stop profiting from such content…Although we attempt to monitor the content posted on Weibo, we may not always be able to effectively control or restrict the content generated or placed on Weibo by our users and the PRC government may increase the level of Internet censorship. (Sina, 2012, p. 7)

The implementation of government-imposed regulations such as the Real Name Registration policy demands significant monetary and labor input, all of which reduces Weibo's profitability. Simultaneously, however, not fulfilling the government's censorship requirements is too big of a risk for the company to take. Indeed, the failure to comply with state laws and regulations will endanger the business license, as Sina states in a recent Annual Report:

> … failure to do so on a timely and adequate basis may subject us to liability and certain penalties given by the State security Bureau, ministry of Public Security and/or the MII or their respective local counterparts. (Sina, 2011)

As a result, Weibo has put in place both computer filtering mechanism and human labor to monitor and police online content. In October 2009, when the microblog service started to become widely popular, Sina invested heavily in developing a content-filtering technology system that it would use to protect the burgeoning microblog product. The management team stated in an interview with the *Wall Street Journal* that: "the political risks associated with the microblog are very high, as it is no longer point-to-point communication but information that is much more rapidly transmitted. Therefore, we need to be cautious in every respect" (Shanshan, 2010). As a result, internet censorship is not only a hard rule that Weibo has to follow in its operation, but is also an integral part of the company's business strategy and its efforts to save costs and increase profit. In Johan Lagerkvist's (2010) interview with a manager at Sina, the latter stated that: "we work very, very closely with the government, the Propaganda Department […] we are not allowed to have our own correspondents. We are dependent on the government for news. It is a good way – saves cost also" (p. 146).

Weibo has also taken further steps to develop mechanisms to police web content and individual users. The User Credit System that was put into effect in 2012, for instance, is an example of such an attempt. The Weibo User Credit System allows users to report on other accounts when they post untruthful information, leak other people's personal information, or copy other people's content. Scores are deducted based on the company's assessment of the seriousness of the complaint. Every user's initial credit score is 80 and when the user's credit score is deducted to 0, the account will be shut down automatically. As a remedy, users can also earn back their scores by doing the following: posting to Weibo everyday earns a user one point every seven days; or they can earn ten points by submitting their personal identification number or linking their cellphone number to their Weibo account. The User Credit System, in short, encourages users to censor their own content and that of others while at the same time encouraging them to offer more personally identifiable information to the service, thus making themselves more identifiable, surveillable and disciplinable. Moreover, earning credit by actively posting to Weibo everyday also achieves the aim of building internet traffic for the service. This User Credit System, therefore, exemplifies how elements of commercial imperatives are being skillfully, and subtly, integrated with incentives for surveillance, censorship and self-censorship.

In sum, Weibo serves as an example of how an online service provider in China manages to comply with the rigid legal and regulatory environment while also succeeding in generating profit and maintaining a positive business outlook. The company operates under the stringent legal and regulatory environment carved out by the state, which basically offloads the responsibility to police content to private internet companies as

required by the *Administrative Measures on Internet Information Services*, as reviewed in Chapter 4. According to this regulation, the consequence of non-compliance for Weibo is economic sanction and possible suspension of its business license. With the stipulation of the *Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks,* Weibo is now required to obtain accurate personal information and retain user data for a period of 60 days.

With the ultimate sanction hanging over its business at all times – the risk of having its business license suspended – Weibo has developed a multifaceted system of control, ranging from the technical aspect to the design of the service. The technical design of the website features prominent visibility of the user contracts that users are obliged to obey. Weibo's Real Name Registration policy and the User Credit System bestow a higher class of citizenship relative to others, so to speak, to those Weibo users who (1) link their cellphones to their Weibo accounts; (2) register using their national identity card and (3) contribute messages and other types of activities to the website. In turn, each of these measures helps generate traffic for the service and greater knowledge of the audience of Weibo users that is useful to the company's advertising sales. Such measures also make Weibo a more effective tool to whom the state has delegated the responsibility to establish subscribers' identity and monitor their behaviour and messages, while retaining data about them that can later be disclosed without a warrant to various government law enforcement and security agencies.

The promulgation of self-censorship effort by the state under the guise of a moral appeal calling on internet users to be "civilized citizens", and the adoption of laws that make spreading rumours and slanderous content over the internet a crime, further

facilitates changes to internet culture and online behavioral norms. They effectively create a legal and normative environment that encourages users to self-censor content to avoid legal sanction. All of such measures are used by the Chinese government both to compel and encourage Sina to monitor and regulate its subscribers while creating a moral and legal climate in line with the government's framing of political, social and cultural conditions in China.

7 Chapter: Conclusion

Introduced during the country's industrialization and economic reform era, the government has actively promoted the use of the internet for nationalistic development purposes. Although earlier power struggles between different government organizations resulted in many uncoordinated initiatives, two major functions with respect to internet regulation have been consistently and clearly articulated throughout the government's documents and official statements about the internet since its earliest days: first, economically speaking, the primary role of the internet is to fulfill the need for economic development and to accelerate the pursuit of industrialization and informationization; second, and politically speaking, the aim has been to develop the internet in ways that help the Party to enhance its organizational efficiency and political legitimacy. Essentially, the internet is viewed as a neutral and value-free technology – that is, in instrumentalist terms – that the government can employ or discard at its disposal. This instrumental view of the internet bears striking similarity to the old philosophy of "Chinese learning as substance, Western learning for practical use" that emerged during the Self Strengthening Movement in the Qing Dynasty when the country struggled to maintain absolute control over telecommunications in the face of foreign encroachment.

Lawrence Lessig (2006) has stated that in controlling the internet, one central question for the government to know is: "who did what, where?" (p. 39). The Chinese government has designed a legal architecture of control that helps them to obtain answers to this question. Through the ownership and licensing system, the government controls who can enter the market and operate an internet business in China. With the data retention rules, information about individual's digital footprint is recorded and stored.

The real identity policies of the past few years tie that content to real people and their 'real identities' in the corporeal world. Through content regulations, the state sets the boundaries of what kinds of activities are permitted/banned online. Internet controls in China, in other words, are all encompassing from the macro level of the economy and state, down to the specific level of individuals, the 'real' identities, and what they do and say online.

The scope and scale of regulation of private internet companies in China is wide and extensive. As Anne Cheung (2006) states, China's legal framework for internet access and usage is achieved by the participation of state and non-state actors at all institutional levels. At the highest levels of the state, the State Council, the Ministry of Information Industry and the Ministry of Public Security loom large on both the national and local levels. The legal framework covers a wide range of internet activities ranging from internet access and publication to internet usage. Although legal and regulatory control is only the tip of the iceberg, these regulations enable and give a legal veneer of legitimacy to a diverse means of control, ranging from distributing criminal and financial liability, licensing and registration requirements, and self-monitoring instructions to non-state actors at every stage of access, from the ISP to the content provider and the end user (ONI, 2010, p. 458). These formalized forms of control are supplemented by a labyrinth of other informal and technical means of control: job dismissals, detention of journalists, technical filtering, and blocking. The reach of the state is thus vast, and the punishments meted out for a sprawling list of wrongdoings harsh and personal.

Online Service Providers that host social networking services, blogs, and websites constitute an integral part of internet users' online experience. They provide important

online services and platforms through which internet users access the internet, publish and distribute web content and interact with each other. However, as much as these platforms provide great potentials for speech and social interaction, they have also become crucial chokepoints at which internet controls are implemented and acted upon (Zuckerman, 2010, p. 72). This is especially true in a country such as China, where OSPs occupy an important and unique role in internet regulation: on one hand, as the gatekeeper for online speech, they have to censor web content at the behest of the government, on the other, as privately owned, profit-oriented, and publicly-traded companies, they have to minimize the negative impact of such actions on the company's profitability, ability to attract users and to stimulate activity on their sites.

The case study of Sina Weibo shows that at least this Online Service Provider acts as the handmaiden of the state under a stringent regime of control. In fear of economic penalty and suspension of its business license, Sina Weibo has constructed an online space that encourages user self-identification and self-censorship. Controls are exerted and enacted in overt manners, such as in the legally binding user contract and in the design of the user interface that features prominent visual cues for users to obey these rules. Controls are also exerted covertly, such as in the User Verification System and Sina Weibo's User Credit System — two mechanisms that, on one hand, enable the company greater ability to control and monitor user activity by harvesting their personal information and data such as cell phone number, while on the other hand, encouraging more web traffic by allowing users to increase their credit score through frequent posting and commenting activities. Although these control mechanisms never achieve perfect control of cyberspace, the Chinese state has been relentless in its bid to delegate

responsibilities for policing online content to private companies, at significant costs to user's freedom of expression.

In sum, by examining how cyberspace controls are enabled in the legal and regulatory realms in China, and often operationized through commercial internet intermediaries, this thesis complicates the common understanding of how internet censorship works in China. Other than harsh internet blocking and filtering – the "Great Firewall of China", internet controls are enacted on a more mundane level in user's daily encounter with online service providers and these control measures cannot be overlooked easily because they are performed and exercised daily. The norms of online participation and behaviors of internet users is thus gradually being adapted and shaped in line with the perceived needs of the state – an outcome that perhaps reconciles state interests with private business objectives but at the expense of citizens, their rights and the overall character of the internet in China. In sum, each of these measures is carving out a distinctly Chinese internet within the overarching global internet.

Bibliography

Arsene, S. (2012). The impact of China on Global Internet Governance in an Era of Privatized Control. *Chinese Internet Research Conference.* Los Angeles.

Bandurski, D. (2013, August 27). *China's "seven base lines" for a Cleaner Internet*. Retrieved April 1, 2014, from China Media Project: http://cmp.hku.hk/2013/08/27/33916/

Bandurski, D. (2006, October 23). *Chinese Media Criticize Proposed "identification system" for Weblogs in China*. Retrieved April 10, 2013, from China Media Project: http://cmp.hku.hk/2006/10/23/114/

Barlow, J. (1996, Feburary 8). *A Declaration of the Independence of Cyberspace*. Retrieved Janurary 22, 2014, from Electronic Frontier Foundation: https://projects.eff.org/~barlow/Declaration-Final.html

Bristow, M. (2008, December 6). *China's Internet "Spin Doctor"*. Retrieved from BBC News: http://news.bbc.co.uk/2/hi/7783640.stm

Chao, E. (2012, November 20). *Five Myths about the Chinese Internet*. Retrieved April 10, 2013, from Foreign Policy: http://www.foreignpolicy.com/articles/2012/11/20/five_myths_about_the_chinese_internet

Chao, L. (2012, March 31). *Sina, Tencent Shut Down Commenting on Microblogs*. Retrieved Janurary 16, 2014, from The Wall Street Journal: http://online.wsj.com/news/articles/SB10001424052702303816504577314400064661814

Cheung, A. S. (2006). The Business of Governance: China's Legislation on Content Regulation in Cyberspace. *International Law and Politics , 38* (1), 1-35.

ChinaITLaw. (2010, January 20). *Administrative Measures on Internet Information Services*. Retrieved May 16, 2014, from China.org.cn: http://www.china.org.cn/business/2010-01/20/content_19274704_3.htm

Chu, W.-c., & Cheng, C.-t. (2011). Cultural Convulsions: Examining the Chineseness of Cyber China. In D. K. Herold, & P. Marolt (Eds.), *Online Society in China: creating, celebrating, and instrumentalising the online carnival* (pp. 21-40). New York: Routledge.

Clinton, H. (2010, January 21). *Remarks on Internet freedom*. Retrieved April 10, 2013, from U.S. Department of State: http://www.state.gov/secretary/rm/2010/01/135519.htm

CNNIC. (2012, June 8). *The Internet Timeline of China 1986-2003*. Retrieved January 8, 2014, from China Internet Network Information Center: http://www.cnnic.cn/hlwfzyj/hlwdsj/201206/t20120612_27414.htm

Crandall, J. R., Crete-Nishihata, M., Knockel, J., McKune, S., Senft, A., Tseng, D., et al. (2013). Chat Program Censorship and Surveillance in China: Tracking TOM-Skype and Sina UC. *First Monday , 18* (7).

Custer, C. (2014, Feburary 4). *The Demise of Sina Weibo: Censorship Or Evolution*. Retrieved April 3, 2014, from Forbes: http://www.forbes.com/sites/ccuster/2014/02/04/the-demise-of-sina-weibo-censorship-or-evolution/

Dai, X. (2000). Chinese politics of the Internet: Control and Anti-Control. *Cambridge Review of International Affairs , 13* (2), 181-194.

Damm, J. (2007). The Internet and the fragmentation of Chinese Society. *Critical Asia Studies , 39* (2), 273-294.

Damm, J., & Thomas, S. (2006). Chinese Cyberspaces: Technological Changes and Political Effects. In J. Damm, & S. Thomas (Eds.), *Chinese Cyberspaces: Technological Changes and Political Effects* (pp. 1-11). Routledge.

Deibert, R. (2003). Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace. *Journal of International Studies , 32* (3), 501-530.

Deibert, R. J. (2013). *Black Code: Inside the Battle for Cyberspace.* Toronto: McClelland & Stewart.

Deibert, R., & Rohozinski, R. (2012). Contesting Cyberspace and the Coming Crisis of Authority. In R. Deibert, R. Rohozinski, J. Palfrey, & J. Zittrain (Eds.), *Access contested: security, identity and resistance in Asian cyberspace* (pp. 21-43). Cambridge, Massachusetts: The MIT Press.

Demers, D., & Merskin, D. (2000). Corporate News Structure and the Managerial Revolution. *The Journal of Media Economics , 13* (2), 103-121.

DeNardis, L. (2012). Hidden Levers of Internet Control: an Infrastructure-based Theory of Internet Governance. *Information, Communication & Society , 15* (5), 720-738.

DeNardis, L. (2010). The Emerging Field of Internet Governance. *Yale Information Society Project Working Paper Series .*

Dong, F. (2012). Controlling the Internet in China: the Real Story. *Convergence: the International Journal of Research into New Media Technologies , 18* (4), 403-425.

Edwards, P. N. (2003). Infrastructure and Modernity: Force, Time, and Social Organization in the History of Sociotechnical Systems. In T. J. Misa, P. Brey, & A. Feenberg (Eds.), *Modernity and Technology* (pp. 185-225). Cambridge: The MIT Press.

Farrall, K., & Herold, D. K. (2011). Identity vs. Anonymity: Chinese Netizens and Questions of Identifiability. In D. K. Herold, & P. Marolt (Eds.), *Online Society in China: Creating, Celebrating, and Instrumentalising the Online Carnival* (pp. 165-184). New York: Routledge.

Feenberg, A. (2010). Democratic Rationalization: Technology, Power, and Freedom. In A. Feenberg, *Between Reason and Experience: Essays in Technology and Modernity* (pp. 5-29). Cambridge, Massachusetts: The MIT Press.

Fu, K.-w., Chan, C., & Chau, M. (2013). Assessing Censorship on Microblogs in China: Discriminatory Keyword Analysis and Impact Evaluation of the "Real Name Registration" Policy. *IEEE Internet Computing.* IEEE Computer Society.

Goldsmith, J., & Wu, T. (2006). *Who Controls the Internet?: Illusions of a Borderless World.* New York: Oxford University Press.

Guo, L. (2007). *Surveying Internet usage and impact in seven Chinese cities.* Chinese Academy of Social Sciences, Center for Social Development.

Hassid, J. (n.d.). The Politics of China's Emerging Micro-blogs: Something New or More of the Same?

He, Z. (1997). A History of Telecommunications in China. In P. Lee (Ed.), *Telecommunications and Development in China* (pp. 55-87). Cresskill: Hampton Press.

He, Z. (1997). A History of Telecommunications in China: Development and Policy Implications. In P. S. Lee (Ed.), *Telecommunications and Development in China* (pp. 55-87). Cresskill: Hampton Press.

Herold, D. K. (2013). *An Inter-nation-al Internet: China's Contribution to Global Internet governance?*

Hu, H. L. (2011). The Political Economy of Governing ISPs in Perspectives of Net Neutrality and Vertical Integration. *The China Quarterly , 207*, 523-540.

Information Office of the State Council of the People's Republic of China. (2010, June 8). *The Internet in China*. Retrieved April 10, 2013, from Chinese Government's Official Web Portal: http://www.gov.cn/english/2010-06/08/content_1622956.htm

IOSC. (2010, June 8). *The Internet in China*. Retrieved Janurary 16, 2014, from China.org.cn: http://www.china.org.cn/government/whitepaper/node_7093508.htm

ITU. (2005, November 18). *WSIS: Tunis Agenda for the Information Society*. Retrieved December 19, 2013, from World Summit on the Information Society: http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

Jacob, A. (2013, September 23). *China's Crackdown Prompts Outage Over Boy's Arrest*. Retrieved May 22, 2014, from New York Times: http://www.nytimes.com/2013/09/24/world/asia/crackdown-on-dissent-in-china-meets-online-backlash-after-boys-arrest.html?_r=0

Jiang, M. (2010). Authoritarian Deliberation on Chinese Internet. *Electronic Journal of Communication , 20* (3&4).

Jiang, M. (2010). Authoritarian Informationalism: China's Approach to Internet Sovereignty. *SAIS Review , XXX* (2), 71-89.

Jiang, M. (2012). Internet Companies in China: Dancing between the Party Line and the Bottom Line. *Asie. Visions , 47*.

Kalathil, S., & Boas, T. (2003). *Open Networks, Closed Regimes: the Impact of the Internet on Authoritarian rule.* Washington: Carnegie Endowment for International Peace.

Karagiannopoulos, V. (2012). China and the Internet: Expanding on Lessig's Regulation Nightmares. *Scripted , 9* (2), 150-172.

King, G., Pan, J., & Roberst, M. (2013). How Censorship in China Allows Government Criticism but Silences Collective Expression. *American Political Science Review , 107* (2), 326-343.

Kluver, R. (2005). The Architecture of Control: a Chinese Strategy for e-Governance. *International Public Policy , 25* (1), 75-97.

Kluver, R. (2005). US and Chinese Policy Expectations of the Internet. *China Information , XIX* (2), 299-324.

Kluver, R., & Banerjee, I. (2005). Political Culture, Regulation, and Democratization: the Internet in nine Asia nations. *Information, Communication & Society , 8* (1), 30-46.

Kluver, R., & Yang, C. (2005). The Internet in China: a Meta-Review of Research. *The Information Society: An International Journal , 21* (4), 301-308.

Lagerkvist, J. (2010). *After the Internet, Before Democracy: competing norms in Chinese media and society.* Bern: Peter Lang.

Lagerkvist, J. (2008). Internet Ideotainment in the PRC: National Responses to Cultural Globalization. *Journal of Contemporary China , 17* (54), 121-140.

Lagerkvist, J. (2012). Principle-Agent Dilemma in China's Social Media Sector? The Party-State and Industry Real-Name Registration Waltz. *International Journal of Communication , 6*, 2628-2646.

Lee, C.-C. (2000). Chinese Communication: Prisms, Trajectories, and Modes of Understanding. In C.-C. Lee (Ed.), *Power, Money and Media: Communication Patterns and Bureaucratic Control in Cultural China* (pp. 3-45). Evanston: Northwestern University Press.

Lee, J.-A. (2012). Regulating Blogging and Microblogging in China. *Oregon Law Review , 91*, 609-620.

Lee, J.-A., & Liu, C.-Y. (2012). Forbidden City Encloused by the Great Firewall: the Law and Power of Internet Filtering in China. *Minnesota Journal of Law, Science, and Technology , 13* (1), 125-151.

Lessig, L. (2006). *Code 2.0.* New York: Basic Books.

Liang, B., & Lu, H. (2010). Internet Development, Censorship, and Cyber Crimes in China. *Journal of Contemporary Criminal Justice , 26* (1), 103-120.

Link, P., & Qiang, X. (2013). From "Fart People" to Citizens. *Journal of democracy , 24* (1), 79-85.

Lubman, S. (2013, September 18). *The "Legalization" of China's Internet Crackdown*. Retrieved March 28, 2014, from China Real Time Report: http://blogs.wsj.com/chinarealtime/2013/09/18/the-legalization-of-chinas-internet-crackdown/

Lugg, A. N. (2013). Mantous and Alpacas As Weapons of the Weak: Chinese spoof video and self-expression online. *First Monday , 18* (7).

Lynch, D. (2000). The Nature and Consequences of China's Unique Pattern of Telecommunications Development. In *Power, Money, and Media: Communication Patterns and Bureaucratic Control in Cultural China* (pp. 179-208). Evanston: Northwestern University Press.

Ma, L. (2013). The Diffusion of Government Microblogging. *Public Management Review , 15* (2), 288-309.

MacKinnon, R. (2011). China's "Networked Authoritarianism". *Journal of Democracy , 22* (2), 32-46.

MacKinnon, R. (2009). China's Censorship 2.0: How Companies Censor Bloggers. *First Monday , 14* (2).

MacKinnon, R. (2012). Corporate Accountability in Networked Asia. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.). Cambridge, Massachusetts: The MIT Press.

MacKinnon, R. (2010). Networked Authoritarianism in China and Beyond: Implications for Global Internet Freedom. *Liberation technology in authoritarian regimes.* Standford University.

Mansell, R. (2003). Political Economy, Power and New Media. *New Media & Society , 6* (1), 95-106.

McTaggart, C. (2003). A Layered Approach to Internet Legal Analysis. *McGill Law Journal , 48* (4), 571-627.

Meng, B. (2011). From Steamed Bun to Grass Mud Horse: E Gao as alternative political discourse on the Chinese Internet. *Global Media and Communication , 7* (1), 33-51.

Meng, B. (2010). Moving Beyond Democratization: A Thought Piece on the China Internet Research Agenda. *International Journal of Communication , 4*, 501-508.

Millward, S. (2013, January 10). *Now China's WeChat App is Censoring its Users Globally*. Retrieved April 10, 2013, from Tech in Asia: http://www.techinasia.com/china-wechat-censoring-users-globally/

Millward, S. (2013, July 11). *Survey Finds That Sina Weibo Users Less Active This Year*. Retrieved April 2, 2014, from TechinAsia: http://www.techinasia.com/sina-weibo-users-less-active-2013/

Misa, T. J. (1988). How Machines Make History, and How Historians (and others) Help Them to Do So. *Science, Technology, and Human Values , 13*, 308-331.

Misa, T. J. (1994). Retrieving Sociotechnical Change from Technological Determinism. In M. R. Smith, & L. Marx (Eds.), *Does Technology Drive History?* (pp. 115-141). Cambridge, MA: MIT Press.

Morozov, E. (2011). Whither Internet Control? *Journal of democracy , 22* (2), 62-74.

Mueller, M. (2012). China and Global Internet Governance: A Tiger by the Tail. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (pp. 177-194). Cambridge, Massachusetts: The MIT Press.

Mueller, M., Tan, & Zixiang. (1997). *China in the Information Age: Telecommunications and the Dilemmas of Reform.* Washington, DC: Praeger.

Muller, M. (2010). *Networks and States: the Global Politics of Internet Governance.* Cambridge, Massachusetts: The MIT Press.

Mumford, L. (1964). Authoritarian and Democratic Technics. *Technology and culture , 5* (1), 1-8.

Nanfang Daily. (2013, August 27). *Di Zhi Wang Luo Yao Yan Shi Mei Wei Gong Min De Ze Ren*. Retrieved March 28, 2014, from Netease News: http://news.163.com/13/0827/08/9796TBCU00014AED.html

OpenNet Initiative. (2009). *China's Green Dam: the implications of government control encroaching on the Home PC*. Retrieved April 10, 2013, from OpenNet Initiative Bulletin: https://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc

Paltemaa, L., & Vuori, J. (2009). Regime Transition and the Chinese Politics of Technology: From Mass Science to the Controlled Internet. *Asian Journal of Political Science , 17* (1), 1-23.

People's Daily. (2005, October 19). *Guo Min Jing Ji He She Hui Fa Zhan Di Shi Ge Wu Nian Ji Hua*. Retrieved May 14, 2014, from People's Daily: http://theory.people.com.cn/GB/40557/54239/54243/3783806.html

People's Daily. (2013, August 26). *Jin Fang Da V Bian Da Yao*. Retrieved May 22, 2014, from People's Daily: http://paper.people.com.cn/rmrb/html/2013-08/26/nw.D110000renmrb_20130826_2-04.htm

People's Daily. (2013, September 9). *Liang Gao <Guan Yu Ban Li Li Yong Xin Xi Wang Luo Shi Shi Fei Bang Deng Xing Shi An Jian Shi Yong Fa Lu Ruo Gan Wen Ti De Jie Shi> Quan Wen*. Retrieved April 1, 2014, from People's Daily: http://legal.people.com.cn/n/2013/0909/c42510-22859612.html

People's Daily. (2012, December 18). *Wang Luo Bu Shi Fa Wai Zhi Di*. Retrieved May 15, 2014, from People's Daily: http://paper.people.com.cn/rmrb/html/2012-12/18/nw.D110000renmrb_20121218_9-01.htm

People's Daily. (2013, November 15). *Xin Lang Chu Li Shi Wan Wei Fan "Qi Tiao DI Xian" Weibo Zhang Hu*. Retrieved April 1, 2014, from People's Daily: http://webcache.googleusercontent.com/search?q=cache:ouYYVSEXKP4J:society.people.com.cn/n/2013/1115/c229589-23556832.html+&cd=1&hl=en&ct=clnk&gl=ca

Poell, T., de Kloet, J., & Zeng, G. (2013). Will the Real Weibo Please Stand up? Chinese Online Contention and Actor Network Theory. *Chinese Journal of Communication*. DOI:10.1080/17544750.2013.816753

PRC. (1997, May 20). *Interim Regulations on the Management of International Networking of Computer Information*. Retrieved May 22, 2014, from World Intellectual Property Organization: http://www.wipo.int/wipolex/en/details.jsp?id=6561

Qiang, X. (2011). The Battle for the Chinese Internet. *Journal of Democracy , 22* (2), 47-61.

Robinson+Yu. (2013, April). Collateral Freedom.

Seltzer, W. (2010). Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of The DCMA on The First Amendment. *Harvard Journal of Law & Technology , 24* (1), 171-232.

Shanshan, W. (2010, July 4). *Sina's Microblogging Power*. Retrieved March 28, 2014, from The Wall Street Journal: http://www.marketwatch.com/story/sina-brings-microblogging-to-china-2010-07-04

Sina. (2012, March 31). *Sina Weibo Gong Gao*. Retrieved March 31, 2014, from Sina Weibo: http://www.weibo.com/z/notice20120331/

Stein, L. (2013). Policy and Participation on Social Media: The Case of YouTube, Facebook and Wikipedia. Communication, Culture & Critique, 6 (3), 353-371

Stockmann, D., & Gallagher, M. (2011). Remote Control: How the Media Sustain Authoritarian Rule in China. *Comparative Political Studies , 44* (4), 436-467.

Sullivan, J. (2013). China's Weibo: Is faster different? *New Media & Society* .

Szablewicz, M. (2010). The Ill Effects of "Opium for the Spirit": a Critical Cultural Analysis of China's Internet Addiction Moral Panic. *Chinese Journal of Communication , 3* (4), 453-470.

Taubman, G. (1998). A Not-So World Wide Web: The Internet, China and the Challenges to Nondemocratic Rule. *Columbia University , 15* (2), 255-272.

The Economist. (2013, April 6). *China's Internet: a Giant Cage*. Retrieved September 23, 2013, from The Economist: http://www.economist.com/news/special-report/21574628-internet-was-expected-help-democratise-china-instead-it-has-enabled

Tsui, L. (2007). An Inadequate Metaphor: the Great Firewall and Chinese Internet Censorship. *Global Dialogue , 9* (1-2).

Wacker, G. (2003). The Internet and Censorship in China. In C. Hughes, & G. Wacker (Eds.), *China and the Internet: politics of the digital leap forward* (pp. 58-83). London: RoutldgeCurzon.

Weber, I., & Jia, L. (2007). Internet and Self-Regulation in China: the Cultural Logic of Controlled Commodification. *Media, Culture & Society , 29* (5), 772-789.

Winner, L. (1977). *Autonomous Technology: Technics-Out-of-Control as a Theme in Political Thought.* Cambridge: MIT Press.

Winner, L. (1980). Do Artifacts Have Politics? *Daedalus , 109* (1), 121-136.

Winner, L. (1986). *The Whale and the Reactor: a Search for Limits in an Age of High Technology.* Chicago: University of Chicago Press.

Wright, J. (2013). Regional variation in Chinese Internet filtering. *Information, Communication & Society , 17* (1), 121-141.

Wu, A. X. (2012). Hail the Independent Thinker: The Emergence of Public Debate Culture on the Chinese Internet. *International Journal of Communication* , 2220-2244.

Wu, T. (2010). *The Master Switch: the Rise and Fall of Information Empires.* New York: Knopf.

Xinhua. (2011, May 4). *China Sets Up State Internet Information office*. Retrieved March 28, 2014, from ChinaDaily: http://www.chinadaily.com.cn/china/2011-05/04/content_12440782.htm

Xinhua. (2013, August 15). *Zhong Guo Hu Lian Wang Da Hui Chang Yi Gong Shou "Qi Tiao Di Xian"*. Retrieved April 1, 2014, from Xinhua News: http://news.xinhuanet.com/politics/2013-08/15/c_116961278.htm

Xue, S. (2005). Internet policy and diffusion in China, Malaysia, and Singapore. *Journal of Information Science , 31* (3), 238-250.

Yang, C., & Kluver, R. (2005). Information Society and Privacy in the People's Republic of China. *Journal of E-Government , 2* (4), 85-105.

Yang, G. (2012). A Chinese Internet? History, practice and globalization. *Chinese journal of communication , 5* (1), 49-54.

Yang, G. (2003). The Internet and the Rise of a Transnational Chinese Cultural Sphere. *Media Culture & Society , 25* (4), 469-490.

Yang, G. (2009). *The Power of the Internet in China: Citizen Activism Online.* New York: Columbia University Press.

Yilun, C. (2014, January 17). *China Weibo Users Drop 9% as Tencent App Competition Grows*. Retrieved April 3, 2014, from Businessweek: http://www.businessweek.com/news/2014-01-16/china-microblog-users-drop-9-percent-as-tencent-app-competition-widens

Yuan, W. (2010). E-democracy@China: does it work? *Chinese Journal of Communication , 3* (4), 488-503.

Zhao, Y. (2007). "Universal service" and China's Telecommunications Miracle: Discourses, Practices, and Post-WTO Accession Challenges. *info , 2* (3), 108-121.

Zhao, Y. (2007). After Mobile Phones, What? Re-embedding the Social in China's "Digital Revolution". *International Journal of Communication , 1*, 92-120.

Zhao, Y. (2010). China's Pursuits of Indigenous Innovations in Information Technology Developments: Hopes, Follies and Uncertainties. *Chinese Journal of Communication, 3* (3), 266-289.

Zhao, Y. (2008). *Communication in China.* Maryland: Rowman & Littlefield Publishers.

Zhao, Y. (2003). Transnational Capital, the Chinese state, and China's Communication Industries in a Fractured Society. *The Public , 10* (4), 53-74.

Zhou, Y. (2006). *Historicizing Online Politics: Telegraphy, the Internet, and Political Participation in China.* Stanford: Standford University Press.

Zittrain, J. (2003). Internet Points of Control. *Boston College Law Review , 43* (1).

Zittrain, J., & Edelman, B. (2003, March/April). Internet filtering in China. *IEEE Internet computing* , 70-77.