

The Political Economy of Governing ISPs in China: Perspectives of Net Neutrality and Vertical Integration

Henry L. Hu *

ABSTRACT Internet service providers (ISPs) have played an important role in China's internet regulation regime. This article illustrates how ISPs are governed to serve the government's regulatory goals. This involves examining some of the most extraordinary and profound insights concerning internet governance: the theories of the layers principle, the end-to-end argument and the generative internet. Chinese ISPs have been dependent rather than neutral regulatory intermediaries of the government. Moreover, in addition to telecommunication carriers, the radio and television networks affiliated to the State Administration for Radio, Film and Television (SARFT) are to become a new type of ISP that is capable of choking the free spirit of the internet, as recently demonstrated by the far-reaching policy of "network convergence." This article argues that the policy has the potential to drastically alter the structure and ecology of the internet in China.

Internet service providers (ISPs) have played an important role in China's internet regulation regime. They can be roughly divided into two categories based on business scale: backbone ISPs and last-mile ISPs. Backbone ISPs own independent gateways connected to the international internet and outsource the final access business to last-mile ISPs. At present, China has seven major backbone ISPs running three commercial networks (China Telecom, China Unicom and China Mobile) and four public service networks (CSTNET, CERNET, CIETNET and CGWNET). This article illustrates how these two kinds of ISP are governed to serve the government's regulatory goals.

Drawing the contours of ISPs' daily operations does not fully explain the intent and logic of internet regulation using ISPs. Any explanation involves some of the most extraordinary and profound insights concerning internet governance – the theories of the layers principle, the end-to-end argument and the generative internet – which to a certain extent justify regulations in favour of net neutrality.

* Shanghai University of Finance and Economics. Email: hulingpku@gmail.com

Although these theories have not been applied in any literature to Chinese internet, I believe they will prove to be powerful tools and useful perspectives to cast light on Chinese internet regulation. Chinese ISPs have been dependent rather than neutral regulatory intermediaries of the government. Their political actions and commercial behaviours can compromise the function of internet as an open and innovative platform for culture production, free expression and creative industry. Moreover, in addition to telecommunication carriers, the radio and television networks affiliated to the State Administration for Radio, Film and Television (SARFT) are to become a new type of ISP that is capable of choking the free spirit of the internet, as recently demonstrated by the far-reaching policy of “networks convergence.” The latent effects of this policy remain ignored by academia. This article argues that the policy has the potential to drastically alter the structure and ecology of the internet in China.

The article begins by summarizing the legal obligations and daily operations of ISPs, with an emphasis on the mechanisms of the Great Firewall. It then sets out the theories of the layers principle, the end-to-end argument and the generative internet, and describes two cases of VoIP and P2P in Chinese context. Based on these, it takes the SARFT as an example to show the problems and regulatory implications of the “networks convergence” policy, identifying a perfect model of internet control without checks and balances.

Legal Obligations of ISPs and the Implementing Regime

The Great Firewall at the national level

In China, ISPs assume heavy and important responsibilities of internet regulation. Both backbone and last-mile ISPs are responsible for online content blocking and filtering. At the national backbone level, the state asks its managing agents to apply blocking and filtering technologies to the international gateways to prevent domestic users from visiting certain foreign sites and foreign users from visiting certain domestic sites. Such action is primarily taken in major cities such as Beijing, Shanghai and Guangzhou, where most international gateways are located. The blocking and filtering hardware and software is known as the Great Firewall (GFW).¹

The GFW is capable of scanning each data package passing through the international gateway and preventing the users from visiting politically sensitive sites or contents, using various measures including IP blocking, DNS filtering and redirecting, URL filtering, packet filtering and denial of service.² The blacklist

- 1 The word first appeared in the title of a 1998 essay in *Wired* magazine (Niall McKay, “China: the Great Firewall,” <http://www.wired.com/politics/law/news/1998/12/16545>), although this has nothing to do with the GFW discussed here. It is widely accepted that the word was first formally used to criticize China’s policy in Charles R. Smith, “The Great Firewall of China,” <http://archive.newsmax.com/archives/articles/2002/5/17/25858.shtml>.
- 2 Jonathan Zittrain and Benjamin Edelman, “Empirical analysis of internet filtering in China,” <http://cyber.law.harvard.edu/filtering/china/>; Steven J. Murdoch and Ross Anderson, “Tools and technology

of sensitive words is arbitrarily decided and revised at times based on the political needs of different central agencies. Renowned sites, especially the social-production sites like Wikipedia, YouTube and Flickr, are always on the blacklist and therefore inaccessible to the Chinese public, because they contain “harmful information” to the government that cannot be controlled by it. The operation of the GFW in the black box is confidential and complicated so that people can only see a tiny fraction of the whole picture from the scarce information gathered by random testing. Netizens have no reasonable expectation about what sites they are allowed to visit and what information they can obtain. In practice, more and more people are aware of the GFW and are bothered by it, although some of them cannot distinguish governmental manipulation from simple technical mistakes. However, only a small number have the incentive to browse “across the wall.”³ For these “tech savvies,” it is fairly easy to circumvent the GFW with free proxies or software that are readily available on the internet.⁴ Those who are politically insensitive can live quite happily with the business and entertainment content provided by domestic sites.

The primary goal of the GFW is to block the free flow of information and facilitate the formation of a “local net” or “intranet.”⁵ The internet is different from telephone and telegraph in that its operation relies heavily on physical facilities and technological code.⁶ By blocking and filtering the international gateway at the national level, the Chinese government has created one basically “clean” virtual sphere in its own hands. Even if Chinese netizens get around the GFW, they are unlikely to be able to spread any blacklisted information domestically on a large scale because of the inspection of last-mile ISPs at the local level.

ISP censorship at the local level

While the GFW is directly managed by the central government, domestic internet censorship lies with local government. Several laws rule that ISPs shall be held

footnote continued

of internet filtering,” in Ronald Deibert (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, MA: MIT Press, 2008). For a later and comprehensive review of Chinese internet filtering practice, see OpenNet Initiative, “Internet filtering in China,” <http://opennet.net/research/profiles/china>.

- 3 Analysis shows that many netizens were more fond of browsing the overseas news republished by others rather than going across the GFW themselves. See Tian Lu and Yao Yao, “The war of GFW,” *Phoenix Weekly*, No. 2 (2009).
- 4 However, the government is still able to order the domestic software manufactures to kill such circumventing software as a virus or malware. For example, Freegate, a popular software among Chinese netizens, is regarded as virus by almost all Chinese antivirus software.
- 5 Jonathan Zittrain, “Be careful what you ask for: reconciling a global internet and local law,” in Adam Thierer and Clyde Wayne Crews Jr. (eds.), *Who Rules the Net? Internet Governance and Jurisdiction* (Washington, DC: Cato Institute, 2003); John G. Palfrey, “Local nets: filtering and the internet governance problem,” http://cyber.law.harvard.edu/publications/2005/Local_Nets.
- 6 Jack Goldsmith and Tim Wu, *Who Controls the Internet: Illusions of a Borderless World* (New York: Oxford University Press, 2006).

responsible for the information security within their own networks, including keeping the original records of user behaviour and reporting to the police, the same obligations as websites.⁷ These obligations elevated the level of self-censorship by ISPs. As in the case of the GFW, local last-mile ISPs apply a blacklist of key words and websites prescribed by local governments to routers or main nodes covering one or more administrative jurisdictions. Since local blacklists vary substantially, the self-censorship regime causes a split of the internet among towns, cities and provinces. In cases of emergency, provincial governments can order a cut-off of communication networks linked with other provinces.

In addition to the state laws and regulations, backbone networks are subject to different governance structures based on their respective natures.⁸ Non-commercial networks (that is, public service networks) are vertically governed by sectoral regulatory authorities such as Ministry of Education and Chinese Academy of Science that also act as the main content regulators. Because of the relatively small number of users, primarily composed of teachers, researchers, students and soldiers, it is relatively easy to exert control.⁹ By contrast, commercial networks are operated by telecom companies and horizontally supervised by the telecom agencies of local governments, while the information flowing over the internet is governed by other special content agencies.¹⁰

The two distinct patterns of network governance correspond to the universal Chinese government structure systems of *tiao-kuai* (条-块, vertical-horizontal). On one hand, the *tiao* (vertical) governance of non-commercial networks by the sectoral regulatory authorities ensures exclusive control over their proprietary networks (primarily in the education sector) including content regulation and technical maintenance. For example, the Ministry of Education can control any information flow among the inside and outside users of the China Education and Research Network and purge any information deemed harmful or illegal at its sole discretion. On the other hand, the *kuai* (horizontal) governance of commercial networks by local telecom agencies demands self-censorship by the ISPs and co-operation in content regulation among local agencies of several sectoral authorities. While backbone ISPs' subsidiaries and numerous last-mile ISPs impose self-censorship over internet content on a daily basis, local telecom agencies co-ordinate periodic "comprehensive strikes" against

7 E.g. Computer Information Network and Internet Security Protection and Management Regulations, art. 10; Telecommunications Regulation, art. 62.

8 It should be kept in mind that the Chinese internet consists of commercial and non-commercial backbones. Commentators often either mix them up or simply ignore the existence of the latter. As a result, they may lose sight of the basic regulatory style of the government and make mistakes when studying, for example, the real name system in university BBS. For more details, see Hu Ling, "The internet infrastructure and its management"; Hu Ling, "Real name system on the internet: origins and practices," *Internet Law Watch*, No. 8 (2007).

9 Hu Ling, "Real name system on the internet."

10 For non-commercial networks' obligation, see Co-ordination Measures of Management on Internet Websites (17 February 2006); for commercial networks' obligation, see Telecommunications Regulation, ch. V.

unlawful internet content among several sectoral regulatory authorities, a distinctive nature of *kuai* governance. In these official comprehensive strikes, ISPs are heavily relied on to implement the clearing of harmful information, spam, virus and malicious software. For example, the Ministry of Industry and Information (MII) will first send a notice to backbone carriers requiring them to deal with the unlawful content within each network. Then the “self-censorship” or internal examination by ISPs is achieved through technologies such as key word filtering, IP filtering of harmful sites and spam senders, closing illegal sites at the request of other government sectors, or certifying users’ information and trusted servers. Finally the ISPs will be assessed according to their behaviour after the campaign.¹¹

It is especially notable that all Chinese content regulators tend to secure absolute control from the pipes to end devices without any check and balance, either vertically or horizontally. As shown below, China’s regulatory approaches to the virtual world are essentially the same as its traditional governance of the real world. This point is crucial to understanding Chinese internet regulation, but the following section first introduces several basic theories of internet governance.

End-to-end Argument, Layers Principle and the Generative Internet

The internet can be viewed both as inter-connected computers and as a set of technological layers. Three decades ago, the basic principles of internet structure were initiated to aid people in constructing future networks. One of the principles was “end-to-end,” proposed by three MIT computer scientists in 1984.¹² This refers to a system device in which “the function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system.” In other words, the conduits within an ideal system design should solely focus on data transmission, leaving data correction and the main functions of the system to end devices. Similarly, in an ideal computer network, the pipes and cables transmitting data should not interfere with the function of end applications. All they need to do is to ensure the correctness and security of information transmission. The end-to-end argument enabled the internet to flourish during the early age of its development, because all innovations can be experimented at the edge of the internet without any interfere from the centre.

The layers principle claims that the internet can be divided into several layers. Each layer should have its own special function and it is inefficient and

11 The Notice of MII on the Special Measures of Legally Striking Internet Pornography (2007). All leading backbone carriers are members of the special striking leading group.

12 J. H. Saltzer *et al.*, “End-to-end arguments in system design,” *ACM Transactions on Computer Systems*, No. 4 (1984), pp. 277–88. For a detailed description of the role of end-to-end argument in the original internet, see Barbara van Schewick, *Internet Architecture and Innovation* (Cambridge, MA: MIT Press, 2010, forthcoming).

problematic to interfere in one layer for the sake of another.¹³ There are usually three layers – content, logic and physical – which form an hourglass model of the internet.¹⁴ The content and physical layers should develop, while the logic layer such as TCP/IP protocol should be kept simple to facilitate data transmission. In this ideal structure, the numerous end users are encouraged to innovate and produce various contents through personal computer (PC) and operation systems at the periphery of the internet, without worrying about being prohibited or blocked. Eventually a generative internet will come into being, creating more and more prosperous economies and cultures in cyberspace.¹⁵ From the viewpoint of freedom of speech, the internet should not be controlled by ISPs as a common carrier for telecommunication. People are entitled to freedom of expression even on the privately owned information networks, because these usually function as part of the national infrastructure.¹⁶ Despite the security problems caused spontaneously by the same structure, such as virus and cyber-attack, the better solution should be to launch reforms at the end device rather than the middle.¹⁷

These theories induced a public policy debate over “net neutrality” in the United States in 2000.¹⁸ With respect to the blocking behaviour of end software applications by several cable broadband carriers (including Madison River and Comcast), the Federal Communication Commission and Supreme Court ruled that cable providers (different from dial-up ISPs) should not resume the liability of common carriers under Title I of the Telecommunications Act of 1996, and therefore were allowed to discriminate end applications and expressions at their discretion. In response, advocates of net neutrality proposed legislation to make sure the internet was neutrally and non-discriminately managed.¹⁹ Besides the Constitutional justification, the debate mainly focused on economic efficiency. Those who favoured net neutrality argued that discrimination by broadband ISPs would destroy an open platform for mass innovation.²⁰ They urged the government to regulate cable ISPs to the extent of providing a basic protection for end innovation. On the other hand, net neutrality opponents

13 Lawrence B. Solum and Minn Chung, “The layers principle: internet architecture and the law,” *Notre Dame Law Review*, No. 79 (2004), p. 815.

14 Lawrence Lessig, *The Future of Ideas: The Fate of the Commons in a Connected World* (New York: Random House, 2001); Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (New Heaven: Yale University Press, 2006); Jonathan Zittrain, *The Future of the Internet – And How to Stop It* (New Haven: Yale University Press, 2008).

15 Jonathan Zittrain, “The generative internet,” *Harvard Law Review*, No. 119 (2006), p. 1974; Lawrence Lessig, “The architecture of innovation,” *Duke Law Journal*, No. 51 (2002), pp. 1783–1801.

16 Dawn C. Nunziato, *Virtual Freedom: Net Neutrality and Free Speech in the Internet Age* (Stanford, CA: Stanford Law Books, 2009).

17 Zittrain, “The generative internet.”

18 Mark A. Lemley and Lawrence Lessig, “The end of end-to-end: preserving the architecture of the internet in the broadband era,” UC Berkeley Law and Economics Research Paper No. 19 (October 2000).

19 For an overview, see Nunziato, *Virtual Freedom*.

20 Tim Wu, “Network neutrality, broadband discrimination,” *Journal of Telecommunications and High Technology Law*, Vol. 2 (2003), p. 141.

upheld a solution of vertical integration of conduits and end-devices, which was in favour of innovation by last-mile ISPs as opposed to innovation by end users. As long as the market of internet access is competitive, they argued, both innovation and efficiency could be fulfilled by vertical integration.²¹ In fact, both sides acknowledged that competition was necessary for a flourishing internet. The fundamental difference between the two sides was how to handle the relationship between upstream and downstream markets, that is, innovation by end users or ISPs.

Net Neutrality in the Chinese Context

The policy implications of these theories include deciding whether the telecommunication carriers should remain neutral for the purpose of promoting values such as culture production, creativity and freedom of speech, or fully compete in the last-mile market in order to promote innovation. A closer look at Chinese internet regulation reveals a third trajectory, against the original intentions of internet architecture. Before evaluating the conflict between regulation and ideal internet architecture in China, this section examines how such conflict happens and where it is going from two dimensions of ISPs' behaviour.

First is the political behavioural pattern. As illustrated above, Chinese ISPs are far from neutral, because the backbone carriers are all state-owned enterprises. The MII and ISPs are mandated by law to co-operate with special content regulators such as the SARFT and Ministry of Culture: they "monitor the harmful information on the internet and harmful SNS with information security technology and the network platform, and punish those websites that run illegal businesses or spread harmful information."²² On a neutral internet where the digital trace of "harmful" information is protected as privacy it would be hard for special content regulators to fulfil their political tasks. However, thanks to the dependent ISPs, special content administrators can easily block data containing sensitive key words and locate the distributors of such data; they can also easily control end users and ICPS by directly controlling these intermediaries. They utilize one layer of the internet to control contents of another. ISPs are key to filtering the huge number of sensitive words on the blacklist. In such circumstances, Chinese ISPs are more political than commercial.²³

21 Christopher Yoo, "Network neutrality and the economics of congestion," *Georgetown Law Journal*, No. 94 (2006); "Beyond network neutrality," *Harvard Journal of Law and Technology*, No. 19 (2005); "Vertical integration and media regulation in the new economy," *Yale Journal on Regulation*, Winter 2002.

22 Opinion of the General Office of CCP Central Committee and the State Council on Further Strengthening the Management of the Internet (2004).

23 One 2007 case in Shanghai manifested such a dilemma. The personal site of the plaintiff, Du Dongjin, was set in a foreign server and blocked by Shanghai Telecom by mistake. Mr Du not only wanted the site restored but also wanted Shanghai Telecom to reveal the secret black list and the blocking mechanism. Of course the court would not give him such an opportunity to challenge GFW and decided in favour of the defendant that the contract between two sides did not "warrant the plaintiff to successfully visit any particular website." See *Civil Judgment of Pudong New District People's Court of Shanghai*

The second dimension is the commercial behavioural pattern. Although ISPs have little incentive to block harmful information,²⁴ they are apt to block technological innovations that may harm their commercial interest or directly compete with their telecommunication businesses.

A well-known example is the Fu Zhou VoIP case of 1998. In 1997, the Chen brothers in Fu Zhou used net2-phone software to provide overseas VoIP service to the public at a much cheaper price than traditional IDD. The police arrested the Chen brothers and seized all their assets at the request of the local bureau of telecommunication, giving the reason of national interest and normal market order. The Chens sued the police in an administrative litigation. Although the trial court dismissed the action on procedural grounds, the court of appeal decided in favour of the brothers that VoIP is essentially a computer information service that is technically different from traditional telephone services, and therefore, according to existing policies, should not be monopolized by the government for its own interest.²⁵ This landmark decision declared the bankruptcy of a telecommunication agency's intention to monopolize VoIP by legal means, but failed to stop the agency from building its de facto technological monopoly.²⁶ Very soon the MII fought back. First, it decided to license all computer information services so that all future innovations would need official approval. Second, directly against the court's decision, the MII ruled that VoIP and fax service through the internet were an exception to information services, thus prohibiting their use by non-official parties.²⁷ Third, though in 2000 it decided to "open" the VoIP service market and began to issue licences, only the five state-owned telecommunication carriers are qualified to obtain such licences.²⁸ The MII also restricted the localities for the VoIP experiment to only a few cities. These restrictions mean that the progress of the VoIP experiment is long and slow, so that it has yet to grow to a mature industry in China after a decade. Meanwhile, private capital is never allowed to invest in VoIP.

Another example involves Peer-to-Peer (P2P), a technology allowing internet users to share files among their PCs directly. It is widely reported that major telecommunication carriers including China Telecom, China Netcom and China Tie Tong have blocked, or limited the speed of, the use of P2P software such as Bit

footnote continued

(2007) Pu Min Yi (Civil) Primary No. 6518, <http://picasaweb.google.com/yetaai/ChinaInternetCensorshipLawsuitAgainstChinaTelecomByYetaai#>.

24 For example, strikes against harmful information might reduce the interests of the users directly and thus the value of their networks indirectly.

25 *Administrative Verdict of Fu Zhou Intermediate People's Court of Fu Jian Province* (1998) Rong Xing Final No. 76.

26 For a comment, see Zhou Qiren, "Thanks to the Chen brothers: comments on the Fu Zhou IP telephone case," in *Shuwang jingzheng: zhongguo dianxinye de kaifang he gaige (Competition Among .Coms: Openness and Competition in the Telecommunication Industry of China)* (Beijing: Sanlian shudian, 2001).

27 Notice Concerning Questions Relating to the Operating Permit System for International Connections Business of Computer Information Networks (18 September 1998).

28 Notice Concerning Opening the IP Telephone Business in our Country (2 March 2000).

Torrent in several cities on the grounds that such software occupied too much bandwidth at the cost of ISPs.²⁹ It is a reasonable concern. However, from the perspective of net neutrality, the ISPs should not block any legitimate innovative software and applications purely for their own sake. It is realized that the productive way to deal with the problem is not to ban P2P software outright, but to increase bandwidth or implement a quality-of-service policy to differentiate users of different bandwidths at different prices. The real danger lies in the carriers' capacity to suffocate any innovations such as P2P that may conflict with ISPs' interest.

It is commonly believed that basic service providers (access business) should be entrusted with more responsibilities than value-added service providers (information business): for example, the former are obliged to ensure fair access and nondiscrimination while the latter do not have such an obligation. The Chinese Telecommunications Regulation of 2000 also divides the telecommunication business into basic and value-added services, but does not impose distinctive duties on the two types of service provider. In addition, the state-owned broadband ISPs are free to provide both basic and value-added service, which brings a monopoly to both upstream and downstream markets. If a value-added ICP has a conflicting interest with them, they can discriminate any content and end-application at their discretion. It is also impossible for lawyers to reason based on the division between broadband provider and dial-up provider as in the US laws.³⁰ The flaws of the Telecommunications Regulation provide an excuse for illegal behaviour such as P2P blocking to take place, and the latest proposed Telecommunications Law still does not make the necessary distinction to solve that problem.³¹ Future practice is still unclear.

Return to the Regulating Model: The Case of the SARFT

Model of perfect control

This section returns to the question posed earlier: what is the regulating model of Chinese internet governance? And what is the role of ISPs in this model? From the perspective of an online-offline parallel, the *tiao-kuai* management regime in the real world is applied to cyberspace. If the parallel only reflected old characteristics of the regime, then a perspective from the nature of the internet could

29 Although the backbone carriers officially denied the accusation, many local netizens found proof and posted it in the forums, e.g. Li Baiqing, "Tie Tong blocked BT officially," <http://www.tianya.cn/publicforum/Content/it/1/324611.shtml>.

30 According to CNNIC, the number of broadband access users has been rapidly increasing since 2003. In mid-2009 there were 346 million, 90% of the total number of Chinese netizens. All ISPs tried to develop their broadband access business and the traditional dial-up access service almost disappeared. The Telecommunications Regulation does not make any distinction between different access technologies and ISPs. See CNNIC, *The 25th Statistical Survey Report on Internet Development in China* (January 2010), <http://www.cnnic.net.cn/html/Dir/2010/01/15/5767.htm>.

31 See draft art. 44.

provide a new theoretical model which is more powerful in explaining the regulatory intent and behaviour of Chinese government.

Because of the prevailing fear of subversion, content regulation and information security are top priorities for Chinese leaders. Special content regulators tighten the restrictions over the objects under close observation. Such intent is not very different from offline practice. Take licensing for example. Every special content regulator tried to license online professional information such as news, publication, videos and games. Through such action, the government can raise the market entry threshold while facilitating the daily supervision and management of these content industries. Once the number of players is limited, the government can maintain absolute influence. For the scattered information and personal sites outside their realm, they can rely on the un-neutral ISPs for help. The easiest way to regulate these chaotic sites is to shut down the sensitive and unco-operative ones for a period of time, especially during important days such as National Day, and this has become a natural political custom for local governments.

However, these means are not enough for special content agencies where the conduit is in the hands of an independent agency. In order to supervise online information and behaviour, the regulators not only need a set of executive staff but have to control the whole information system as much as possible. Each execution of power involves the platform, infrastructure, standard, market and information, that is, all layers of the internet. Because the information about regulatory objects can be collected through the network platform, it is natural for the regulators to establish their own management system.

In addition, co-operation between different agencies usually involved high transaction costs including refusal to co-operate. This explains why the central government launched the comprehensive movements one after another. If the internet did not exist, or the number of websites grew slowly, or all websites were clearly classified by contents and licensed by different regulators, the business of regulation would have been much easier and more efficient. However, the convergence nature of new media makes it difficult, if not impossible, to control online information in a traditional way. But the regulators' partial interests make them reluctant to deregulate. Thus the establishment of an independent information system is the best way to solve the co-operation problem.

In the digital age, if all the points of information flow are controlled by the same hand, the situation so formed is vertical integration, the same strategy applied by the ISPs. Through this, the regulator can supervise the information flow at any point. It is obvious that such an idea emerged in the minds of Chinese leaders of different agencies. The ideal situation is for the state to control a vertical closed system, which not only brings huge profits from the monopoly industries and prevents intervening from other agencies, but also enables it to enhance the information security protection and construction of the content industry. It will own the power to set rules on industry standard, management

platform, market entrance, regulatory object information and service to the end product. Once state power is combined with commercial interests without any check and balance, corruption can easily occur. Worse, the whole idea of market, free expression and common creativity is censored through the infrastructural control. Unfortunately, China is undergoing such a process and moving fast towards an uncertain future. Such an evolutionary trajectory is shown clearly in the developing process of the radio, film and television industry. The practices of the SARFT exemplify perfectly the policy of vertical integration over the internet.

The problem of the SARFT

The SARFT is a special content regulator which used to control a considerable proportion of people's spiritual products in the history of People's Republic of China. Such control is mainly achieved by tight censorship and active propaganda.³² From the early 1980s, the broadcasting department underwent the same commercialization reform as other media regulators.³³ Local governments have the power and incentive to build their own radio and television networks (RTNs). They also invested in television programmes, especially satellite and cable TV, to promote local economic interests. At that time, the SARFT was still capable of exerting considerable control over the contents conveyed in local RTNs by issuing injunctions to ask local radio or television stations to stop playing indecent or illegal programmes *ex post*.

The internet brings great challenges to the SARFT. One challenge comes from the netizens. The internet empowered ordinary people with generative tools to create their own amateur culture without official gatekeeping and censorship as in the professional cultural production industry. The multiple online channels for videos broke the uniform authority of the SARFT. It became difficult for it to regulate the contents transferred through the internet as compared to traditional RTNs. The SARFT's responses included licensing the special video sites, raising the market threshold through controlling the source and amount of venture capital, and launching special strikes all over the country. However, because the video sites are directly connected with the commercial ISPs, the SARFT can only ask them to conduct self-censorship and hence it can only impose limited influence on them.

The other challenge comes from the ISPs and the MII. In the late 1990s, many ISPs saw great profit in IPTV, a kind of innovative business that combines television broadcasting and interactive services on a uniform platform, which is more

32 For more discussions of the SARFT's role, see Yuezhi Zhao, *Media, Market, and Democracy in China: Between the Party Line and the Bottom Line* (Urbana: University of Illinois Press, 1998); Irene S. Wu, *From Iron Fist to Invisible Hand: The Uneven Path of Telecommunications Reform in China* (Stanford, CA: Stanford University Press, 2009), ch. 3.

33 Daniel C. Lynch, *After the Propaganda State: Media, Politics, and "Thought Work" in Reformed China* (Stanford, CA: Stanford University Press, 1999).

convenient for the audience than traditional one-way television broadcasting. The telecommunication carriers began to build digital video platforms and provide radio and television services on the internet through P2P technology before any relevant regulation came out. Besides great profit, another reason to invest in IPTV is that the nascent online content market was small. The ISPs were seeking new business opportunities to attract more users. Nothing could be more attractive than IPTV, while such business of course infringed the monopoly interests of the SARFT.

Ownership of the communication network plays a vital role in regulatory games in China. It has been well established that ownership of the mass media weighs much in content selection and the formation of public opinion. It can even affect the values of freedom of speech and democracy.³⁴ The problem remains the same in the digital age. Although ordinary people are empowered with the ability to challenge the large incumbents, the latter still have the power to dominate public discourse by means of vertical integration of mass media. In the United States, the danger of convergence of the three layers of the internet has been recognized, but it is difficult to advance the net neutrality principle immediately.³⁵ In China, such ownership also matters, although it is used in different ways. The telecommunication infrastructure has been state-owned from the beginning for reasons of information security and monopoly interest. At the national level, backbone ISPs are supervised by the MII, while the last-mile ISPs are under the supervision of local authorities. Because the MII is not responsible for any content regulation and is mainly in charge of technological and business issues, it lacks the incentive to regulate the end users unless their behaviour threatens economic interests. However, agencies such as the SARFT perform a three-fold task: to promote socialist culture, to make a profit through the RTN, and to defeat harmful information and contents. It has to control the RTN from the conduit to end device for its own sake. If the network was taken away from the SARFT to a more “neutral” agency like the MII, it would lose quite a lot of profit and power. That is why the SARFT always opposes any proposal to let the MII take over the RTN, although the MII could make it more efficient and profitable.

During the telecommunication reform of 1998, the proposal of “convergence of three networks” (*san wang heyi* or *san wang ronghe* 三网合一或三网融合) was first put to the decision makers in the State Council. “Three networks” refer to the telecommunication network, RTN and the internet. The policy goal is to put all three together technically and build a uniform network supporting telephone, video, email and various kinds of communication. The advantage of such a plan is to avoid low-level repeating construction and waste of resources,

34 C. Edwin Baker, *Media Concentration and Democracy: Why Ownership Matters* (New York: Cambridge University Press, 2007).

35 Lessig, *The Future of Ideas*; Mark Cooper, *Media Ownership and Democracy in the Digital Information Age* (Stanford, CA: Center for Internet and Society, Stanford Law School, 2003).

to make full use of digital technology and broadband, and to provide more high quality services and programmes. Obviously, the MII has mastered advanced information technologies and has the incentive and advantage to embrace the RTN to a uniform network. It can easily combine the telecommunication and computer networks together, and this was launched through its 3G plan in 2009. But the reform in the radio and television system has fallen behind because of the large bureaucracy and its disadvantageous technology.

The history of conflict between the SARFT and the MII

The conflict between the SARFT and the MII began at the end of the 1990s. The ISPs were taking advantage of IPTV, as a result of which the SARFT became irritated and refused to co-operate with them. Very soon the provision of IPTV service was prohibited by a joint regulatory document issued by the SARFT and the MII. However, when the MII was established in 1998, a certain amount of the SARFT's authority was transferred to it, especially the power of planning, managing and setting technological standards of the television network, both wire and wireless.³⁶ The SARFT decided to ignore these arrangements and has kept control of the relevant power up to the present. In October 1999, it issued another notice confirming that "any radio, movie and TV programme transmitted through various information networks (including the internet) within the national territory must be submitted to the SARFT for approval."³⁷

In reality, the practices of all kinds of IPTV could not be banned completely because users preferred it to the traditional television set in both its broadcasting speed and its high quality. Local governments also supported such creative business because it brought huge profits.³⁸ As the ISPs began to upgrade the telecommunication networks to broadband conduits, IPTV was welcomed even more. The SARFT had no choice but to build robust digital networks itself to compete with the ISPs. On the one hand, under the shelter of content security, the SARFT tried hard to develop digital television (DTV) networks to replace IPTV in spite of a series of difficulties such as money, the uniform digital technology standard and lack of co-operation from local agencies.³⁹ On the other, it issued several regulations on video sites to restrict online programmes through

36 The Notice of the General Office of the State Council on Strengthening the Management and Construction of RTN (26 June 1998).

37 The Notice of The SARFT on Strengthening the Management of Radio, Movie and TV Programmes through Information Networks (October 1999).

38 In practice, there are three typical models for IPTV, developed in Shanghai, Hangzhou and Qingdao respectively. For a critical review, see Yu Hui *et al.*, "Study on the regulatory policy of convergence of networks," in Yu Hui (ed.), *Gonggong zhengce yanjiu baogao ji I (Collections of Public Policy Research Report I)* (Hangzhou: Zhejiang University Press, 2008), pp. 36–48.

39 Zhou Yan, *Zhongguo shuzi dianshi chanye zhengce de xingcheng yanjiu (Study on the Formation of the Policy of the Digital TV Industry in China)* (Beijing: Communication University of China Press, 2007); Peng Jixiang (ed.), *Chinese Television in the Age of Digital Technology* (Beijing: Peking University Press, 2008), pp. 198–201. Obviously, DTV is less competitive than IPTV, because the latter has many more users.

direct licence, thus indirectly restricting the programme providers from supplying IPTV providers with high-quality video programmes.⁴⁰

To counteract its disadvantage in technology and money, the SARFT could base its strategy on the fact that it continued to control both the end content and the conduit in the name of ideological threats brought by foreign capitals after China signed the WTO agreement. The whole regulatory regime of the SARFT gradually emerged based on the architecture of the internet. Besides tight control over the content transmitted on video sites and the restriction of the market scale of video sites, the authority also realized the advantages of the end broadcasting device and the internet television station. In 2004, the SARFT issued new regulations on online video and programmes in order to comply with the new Administrative Licence Law, which replaced the old one issued only one year previously. The new rules not only strengthened the system of administrative licences but emphasized that “to transmit programmes through the international internet by prefecture-level radio and TV stations is encouraged.”⁴¹ Those ICPs or ISPs running an “internet TV station” without licence from the SARFT would be prohibited and sanctioned. And the internet companies might never be able to obtain a licence for the special end-device for internet television (a TV set-top box) because, according to another rule in 1999, such end-device could only be manufactured by the radio and television stations licensed by the SARFT.⁴² This meant that telecommunication companies could not run IPTV through a TV set-top box but only through a PC, while the radio and television companies could run both businesses. As a result, DTV has become a powerful competitor to IPTV with the latter put at a disadvantage.

It is traditionally convenient and profitable for radio and television agencies to control everything from transmitting conduit to broadcasting end-devices to the content itself. However, several serious problems still exist for the future development of RTNs. The monopoly interests make it impossible to realize the long-term policy goal of the separation of broadcasting network and television station; the RTNs do not have an independent international channel similar to the telecommunication carriers and are restricted from the telecommunication business by the MII; and local agencies are too scattered to form a uniform national network to enhance the competitive capability of the whole industry.⁴³ Although the

40 The SARFT has strictly controlled the creation, aggregation and broadcasting of video programmes, especially the barrier against foreign capital. When Rupert Murdoch’s effort to enter China was about to succeed after ten years’ struggle in around 2004, the new ideological policy of the Hu Jintao era changed to be hostile again. The SARFT was afraid that video online sites could become another form of TV programme and could co-operate with the IPTV industry and circumvent the regulation.

41 Measures for the Administration of the Publication of Audio-Visual Programmes through the Internet or Other Information Network (2004), art. 5.

42 Provisional Management Measures of Approving the Internet Broadcasting End-device (12 November 1999), art. 4.

43 Board of *Caijing Magazine* (ed.), *Guangzhi de huanghun (The Twilight of Regulation)* (Beijing: Social Science Documentation Press, 2003).

SARFT has been advancing DTV network for years, there is no sign that it would regulate the digital network in the same way the MII regulates the internet. It was waiting for an opportunity to build a uniform digital propaganda network all over the country, that is, a proprietary information infrastructure.

Convergence of networks and its regulatory implication

Fortunately, the attitude of the state has gradually changed from prohibiting the SARFT and the MII from running each other's business to encouraging them both to use information technology to provide a digital radio and television service. That means the state decided to pick up the convergence of networks policy to deepen cultural and media reform. After this policy was written into the Eleventh Five-Year Plan in 2005, six ministries jointly issued a milestone document at the beginning of 2008, "Several Policies on Encouraging the Development of the Digital TV Industry," which required speeding up the convergence of three networks substantially. The document stated:

Under the precondition of ensuring the secure transmission of radio and TV programmes, a service and management system fit for developing the convergence of three networks should be established and improved. The radio and TV institutions should be encouraged to provide DTV and value-added telecommunication service through the national public communication network and RTN. Under the precondition of satisfying the finance policy, the investment in the construction of DTV access and the reconstruction of end-device digitalization by national capitals including national telecommunication firms should be supported.

At the same time "the SARFT should tighten the supervision and regulation over the process of producing, aggregating, and broadcasting of the digital programme and make sure the rightness of content and security of broadcasting." In January 2010, the State Council decided to speed up the convergence project, planning to accomplish it in 2015.

These words reveal the very essence of network convergence policy. Obviously it reconciles the conflict and partial interests of the SARFT and the MII. First, a consensus has been formed among the leaders that the country needs network convergence to enhance its international competition and that policy should not be impeded by the narrow interest of agencies. Both the SARFT and the MII (especially the former) realized the advantage of convergence technology and the importance of financial supports from the State Council. Second, the concrete steps of the policy include allowing the SARFT to use telecommunication networks and permitting the MII to invest in digital RTN construction, that is, entry into each other's infrastructure.⁴⁴ Third, the SARFT could gain sufficient

44 According to some sources, the slow speed of the SARFT to advance DTV made the state realize that the status quo without competition must be changed and decide to introduce capital from ISPs into the new industry to advance the overall transformation of DTV. See Luan Lu, "Encouraging DTV industry to develop, telecommunication and broadcasting industry enter into each other from quitting from each other," http://news.xinhuanet.com/fortune/2008-02/03/content_7558403.htm. However, according to the State Council, there are obvious differences between the entitlements of the SARFT and MIIT. The former is encouraged to engage in the telecom business with no limitations while the latter is encouraged to

funding to develop its own digital network and incorporate the scattered local RTNs, which will greatly enhance its power to supervise its subordinates. In the meantime it could maintain its power over the network under the cover of content security and will never give up the chance to develop its own technology standard. That is why it insisted that convergence of networks is not necessarily equal to one uniform network; rather, there could be several technically convergent networks supervised by different agencies. Fourth, the two competitors have different strategies to embrace the technology and policy: the SARFT is developing the Next Generation Broadcasting Network in co-operation with the Ministry of Science and Technology and intends to build it into a fundamental infrastructure covering most of the cities, while the MII (now the Ministry of Industry and Information Technology, MIIT) has finished the 2008 reform, ending up with three telecommunication enterprises, and issued three 3G licences, which also helps solve the VoIP problem. It is reported that the two agencies are co-operating to discuss how to develop the cell phone television,⁴⁵ which seems to break up the contradictions between them. But it is still uncertain how the mobile television and its content will be regulated. The battle over the infrastructure has far from ended.⁴⁶

More interesting is the SARFT's regulatory model, assuming it finishes its DTV plan and dominates the network convergence business. Ideally, the original one-way transmission network would be technically upgraded into a two-way network, all television programmes would be transferred in digital forms and the end-device would be more like a PC than a television set. It is even proposed that an independent institution like the US Federal Communication Commission should take charge of the new media and network.⁴⁷

However, the real effects of such a digital revolution in broadcasting are doubtful, because this ideal would require the SARFT to abandon more power over the RTN. In the future, the RTN might become a new type of ISP quite different from the present ones, probably even stricter, considering that the underlying intent of the SARFT is to enhance its own power and interest in the business of propaganda.⁴⁸ It can of course provide internet access services to customers

footnote continued

engage only in radio and TV *creation* and *transmission* businesses, which is just one aspect of the radio and TV business. The power of editing and broadcasting still remains in the hand of the SARFT.

45 Nan Fang Daily, "Network convergence speeds up; the SARFT engages in cell phone industry," http://media.nfdaily.cn/content/2009-10/21/content_6056088.htm.

46 The deadlock was broken in Jiang Su province as an experiment in July 2009. See "Network convergence might proceed asymmetrically," http://www.21cbh.com/HTML/2009-8-5/HTML_KRVTXCTRRNR.html. Some commentators have doubts about the competitiveness of SARFT: see Xie Wen, "Three problems concerning network convergence," *New Century*, No. 4 (2010).

47 Yu Hui *et al.*, "Study on the regulatory policy of convergence of networks," pp. 54–56.

48 Wang Taihua, head of SARFT, has another higher position in the Party system, that of vice-minister of CPD. Another vice-minister, Cai Wu, also holds a government position, head of the State Council Information Office. This means that the voice from these two ministries is more powerful and effective than other special content regulators, and they are less unlikely to be transformed into one market player.

combined with its rich programme resources, making the IPTV industry more profitable and monopolistic. The convergence technology is only a tool to improve transmission capacity. The SARFT could certainly refuse any institutional change that might threaten its control over the industry standard, transmitting network, end-devices and contents within radio and television broadcasting. It is true that it is much safer to produce a new DTV set, which can satisfy the needs of a mass audience while maintaining tight control of information. Besides, the reforms separating RTN and TV stations, and separating broadcasting and the creation of programmes have all encountered many obstacles all the years. If the relevant reform of the offline media industry cannot succeed, its online counterpart will probably face the same fate. It is highly possible that the future DTV machine is not a generative PC but only an intelligence box; and the future digital RTN is an intelligent and centralized conduit rather than a generative internet. The vertical integration of the digital network and unique end-device would empower the SARFT greatly, facilitate its regulation, restrict entry into the market, and restrict innovation and expression over the network. That is a really perfect model of internet regulation in China.

Conclusion

This article stresses the crucial role of ISPs in Chinese internet regulation. It provides a fresh perspective in observing, as well as a powerful explanation of, the complicated and sometimes disordered regulatory practice in China. Against the background of the *tiao-kuai* regime, it draws a trajectory of cyberspace regulation. The state has tried to incorporate the internet into the traditional administrative framework of media and press (a vertical-horizontal division, which is suitable for a vast country that is politically centralized like China), and make the technological innovation of the internet serve the country's developmental goals. However, it has encountered unexpected difficulties in its efforts to do so, because the internet is different from traditional offline media in its capability of information aggregation and convergence. The theories of layers and generative internet have revealed the secret of maintaining control in the digital age: vertical integration, that is, the state controls not only the end-device and innovative platform but also the conduit for information flow. All relevant sectoral regulatory authorities, such as the Ministry of Culture, are tempted to develop their own methods towards vertical integration. As a result, Chinese ISPs become managing tools for heavy regulation rather than neutral service providers. The debate about net neutrality in the United States focuses on striking a balance among efficiency, equality and freedom of speech. By contrast, the values of net neutrality are never considered in China's policy-making process. No effort to separate the network from the end devices and websites would be successful.

In particular, the SARFT, a content regulatory authority and propaganda agency, is striving to dominate the internet's vertical integration according to the network convergence policy. In the spirit of good governance and net

neutrality, the SARFT is supposed to deregulate the transmission network and focus on end devices. However, the agenda of deregulation will become even more remote if the SARFT transforms the existing radio and television networks into a powerful digital network and becomes the first almighty content regulator of a vertically integrated system. Consequently, the radio and television networks affiliated to the SARFT will become the largest commercial ISP in China. Confronting the double pressures from ideology security and commercialization in the digital era, the SARFT finally explored a way to manage challenges from the internet. It is now not only capable of controlling the content through licences but also has its own special digital network. Such a vertical integration model is the dream of those who possess a monopoly and want to control its content without it being distorted or misused, whether it is political or commercial. There is no doubt that the free spirit of the internet stands to suffer.

To retrieve a more generative and innovative internet based on an open and neutral platform, the future Telecommunications Law should further stipulate different providers' responsibility and establish the common carrier doctrine as the first step. The backbone carriers should not discriminate the legal content transferred in their conduit and applications used on PC and operation systems. A strong and independent judiciary is also needed. At present, because the content regulators do not own the whole network, the extent of control could be buffered; and the effects rely more on co-operation between the MIIT and other regulators. Such labour division ensures the freedom of the present internet to some extent, although ISPs are still participating in content filtering and blocking.