Internet Filtering in

China

OpenNet Initiative
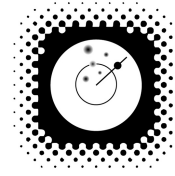
Overview

China has devoted extensive resources to building one of the largest and most sophisticated filtering systems in the world. As the Internet records extraordinary growth in services as well as users, the Chinese government has undertaken to limit access to any content that might potentially undermine the state's control or social stability by pursuing strict supervision of domestic media, delegated liability for online content providers, and increasingly, a propaganda approach to online debate and discussion.

Background

The convening of the 17th Chinese Communist Party (CCP) Congress in October 2007, at which China's top echelon of government leaders chose their eventual successors, was the beginning of a momentous year for China, and consequently for domestic and international news media. On March 10, 2008, hundreds of monks in the Tibetan autonomous region led a series of protests to demand loosening of restrictions on religious practices and

even independence for Tibet.[1] Chinese authorities rapidly responded with arrests and a violent crackdown against thousands of monks and rioting Tibetans.[2] A corresponding clampdown on reporting from the region and other Tibetan-populated areas in western China left media with a dearth of reliable information. With only official accounts and dispatches released by Tibetan exile organizations, issues like the actual death toll were questioned. The crackdown in Tibet galvanized protests both supportive and critical of China's policies towards its religious and ethnic minorities, especially as symbolized in the Olympic torch making its way in an

RESULTS AT A GLANCE					
Filtering	**No evidence of filtering**	**Suspected filtering**	**Selective filtering**	**Substantial filtering**	**Pervasive filtering**
Political					●
Social				●	
Conflict/security					●
Internet tool				●	

Other factors	**Low**	**Medium**	**High**	**Not applicable**
Transparency	●			
Consistency			●	

elaborate tour around the world. The conflicts that erupted in cities as distant as Paris[3] and Seoul in March and April contributed to a so-called transnational Chinese backlash against western media portrayals of China, culminating in a an "anti-CNN" movement and a call for a boycott against the French supermarket chain Carrefour.[4]

On May 12, 2008, a 7.9-magnitude earthquake, with its epicenter in Wenchuan county, Sichuan province, killed around 90,000 people and injured hundreds of thousands, leveling over five million buildings and leaving millions homeless.[5] During the massive relief efforts and national mobilization of volunteers and monetary contributions immediately following the quake, media were allowed to operate with unprecedented openness, with official state outlets such as China Central Television winning notice and praise for presenting timely and uncanned news. However, within a few weeks authorities had already begun to encircle and regulate the story. The government issued bans on coverage of certain topics and required the registration of reporters, but it took authorities repeated efforts to quash coverage of one of the most potent and enduring controversies: the extent of government responsibility for the shoddy

school construction that caused the tragic deaths of thousands of schoolchildren and teachers.[6] Authorities did not release an official statistic of the number of schoolchildren who died until almost a year after the quake, and some accused the official figure of 5,335 figure as too low in comparison with Reuters' estimation of 9,000 deaths, calculated from reports by the state news agency and local media.[7] This led one commentator to state that, "Chinese news reports on this major story unfolded in a complicated environment, and it is impossible to render a simple verdict about media coverage."[8]

With over USD40 billion spent on hosting the 2008 Olympic Games in Beijing, the Chinese government acted to assert control over this global event while presenting an open and welcoming environment for athletes, media, foreign dignitaries and visitors.[9] As part of these overtures, the government issued regulations in January 2007 allowing journalists to travel across the country without registering with local authorities and to interview subjects without official consent.[10] While the unblocking of Web sites and improved access to officials at Olympics venues marked some improvements in openness and transparency, the government also

stepped up surveillance around Beijing and prevented activists from petitioning to use legally sanctioned protest zones.

After a news conference held by the US men's volleyball team, in which several Chinese reporters had their notebooks (and at least one tape recorder) confiscated, Beijing Olympics spokesman Sun Weide denied knowledge of this differential treatment of Chinese reporters: "I am not very clear about the situation you raised," he said. "For Chinese journalists, they very much enjoy the rights to cover the Beijing Olympic Games... the rights are protected by the constitution in China."[11] Yet China's 'open-door' policy for journalists as a result of the Olympics had a marginal impact on Olympics coverage by domestic media. The government persisted in its clampdown on local Chinese media,[12] and the Foreign Correspondents' Club of China confirmed 63 cases of reporting interference during the Olympics out of a total of 178 in 2008, including ten incidents of police roughing up reporters and breaking their cameras.[13] While the relaxed rules for foreign journalists were made permanent in October 2008,[14] new rules issued in February 2009 required reporters based in Hong Kong and Macao to apply for a permit prior to ever reporting trip to mainland China.[15]

A month after the Olympics concluded, a scandal erupted over tainted milk products that killed six infants and sickened nearly 300,000 others.[16] Information soon emerged indicating that provincial governments, central government agencies, as well as officials from the Sanlu group, China's leading seller of milk powder, had either suppressed earlier reports of contamination or failed to act, likely at the cost of human lives.[17] Although it had

been receiving complaints about its infant milk powder since December 2007, the Sanlu group only informed its board in August 2008, prompting its joint venture partner Fonterra to inform the New Zealand government.[18] A reporter for the newspaper Southern Weekend, known for its investigative reports, wrote in a blog post that he several journalists were prevented in July from publishing findings about how milk powder was making children sick because of pressure from Sanlu officials as well as an overall Olympics-related clampdown on negative news coverage.[19] In January 2009, 21 defendants were convicted for their roles in the production and sale of melamine-tainted products, including two melamine producers who received death sentences, and life imprisonment for the former Sanlu chairwoman.[20]

As 2008 progressed, the Chinese government demonstrated a perceptible shift in its media control policies in order to better manage the handling of negative news reports, which continued to spread with incredible speed and intensity on the Internet. Also known as "Control 2.0," this approach involves the government taking a more active and rapid response to fast-breaking news events, primarily by attempting to set the agenda for coverage rather than suppress it.[21] With lessons learned about the upsides of transparency and timeliness from the early Sichuan earthquake coverage and other emergencies, the central government reportedly began allowing local governments to disclose information about unrest and protests in an apparent attempt to "control the news by publicizing the news."[22] However, despite gestures towards a broader openness with the media, the government clearly did not intend to relinquish control.[23] "Control 2.0" often resulted in the same delivery of

"authoritative" facts, with state news agencies such as Xinhua and the People's Daily benefiting from this selectively enhanced coverage over commercial media.[24] In February 2009 the official China News Service announced that it would create a "blacklist" of journalists engaged in "unhealthy professional conduct," and those found breaking rules would be prohibited in news reporting and editing work.[25]

Coming off of these perceived triumphs and devastating crises, the Chinese government warned that extra vigilance was needed in 2009. The potential for increased social instability triggered by the global financial crisis increased anxieties in a year already punctuated by powerful anniversaries of events tainting the legacy of the CCP, which will also commemorate sixty years since the founding of the People's Republic of China: twenty years since the June 4, 1989 Tiananmen Square crackdown; fifty years since the Tibetan uprising that led to the Dalai Lama's exile; and ten years since the Falun Gong spiritual movement was banned quickly after their 10,000-strong flash protest in front of Zhongnanhai, the compound of the Chinese central leadership. Thus, officials repeatedly issued reminders that "stability preservation work"[26] would be a top priority. At a media forum in January, an official in China's Internet affairs bureau said, "[y]ou have to check the channels one by one, the programs one by one, the pages one by one … You must not miss any step. You must not leave any unchecked corners."[27] Efforts to enforce stability preservation have resulted in predictable crackdowns on media reporting; for example, in March 2009, reporters were detained, turned back, or had their recordings confiscated when trying to visit Tibetan areas in three

provinces ahead of the first anniversary of the unrest in Tibet.[28]

Internet in China
China leads the world with 298 million Internet users, an increase of 42 percent from 2007 to the end of 2008.[29] More astoundingly, in this same time period over 90 percent of these users had broadband access, a spike of over 100 million.[30] China also has the world's biggest cell phone market, with some 583.5 million subscribers.[31] The rural-urban divide that influences many gaps in the informatization of the national economy is closing, but remains substantial. With a national Internet penetration rate of 22.6 percent, rural areas and the poorer western provinces are beginning to gain ground.[32] At the end of 2008, rural Internet users made up almost a third of the entire online population, a jump of over 60 percent.[33] While many of the poorer and western provinces such as Yunnan, Gansu and Guizhou continue to have penetration rates of less than 10 percent, they also have considerable growth rates, upwards of 50 percent.[34] Driven by the policy goal that "every village has access to the telephone and every township has access to the Internet" by 2010, infrastructure development has expanded broadband Internet access to 92 percent of townships.[35] Gender is also an important demographic factor in the urban-rural divide, with rural male users significantly outnumbering women by 15 percent. Internet users between the ages of 10-19 gained ground in 2008, increasing to 35 percent of all users and overtaking the 20-29 age group to become the leading demographic using the Internet.[36]

Web sites registered in China are another exponential growth area, increasing by 91.4% from 2007.[37] Social media

platforms continues to take hold: 210 million Internet users in China have visited video sharing sites, 54 percent have blogs (although only 35 percent of those update them at least once every six months), almost a third participate in online discussion forums, and 19 percent belong to social networking sites.[38] Chinese netizens have access to a wide variety of well developed Internet platforms for the domestic market that have typically outpaced foreign services such as search engines (Baidu's market share is at 63 percent compared to Google's 28 percent), online portals (the top four portals – Sohu, Sina, Tencent, and Netease – claim 73 percent of sector revenue), bulletin board services (BBS) and discussion forums, online video sites, blogs, social networking (the service Kaixin has an estimated thirty million daily users), and booming business-to-customer e-commerce.[39] From 2006, when only China Netcom and China Telecom were permitted to offer pilot commercial VoIP services in selected cities,[40] the number of VoIP service providers has reached 3,000, mainly in Beijing and Shanghai, with the number of users reaching 80 million.[41]

In 2008, China's telecom regulator, the Ministry of Information Industry (MII), was dissolved and its functions absorbed into the new Ministry of Industry and Information Technology (MIIT).[42] In addition to the MII mandate to regulate telecommunications, Internet, broadband, electronics, computing and software, the MIIT's enhanced authority includes supervision of IT development, formerly held by the National Development and Reform Commission.[43] Physical access to the Internet is controlled by the MIIT and is provided by eight state-licensed Internet access providers (ISPs), each of which has at least one connection to a foreign Internet backbone.[44] China's international outlet bandwidth reached 640Gbps in 2008, an increase of 73.6 percent, but China Telecom (ChinaNET) maintained over 50 percent of that bandwidth.[45] China Netcom (now China Unicom) joined China's second largest ISP, China169, after China Telecom split off in 2003.[46]

In an effort to boost the fixed-line phone industry's competitiveness in the mobile market, in 2008 numerous ministries jointly decided to merge the assets of the nation's six state-owned telecommunication companies and form three groups in 2008, announcing a plan to issue licenses for high-speed 3G cell phone services after the restructuring.[47] As part of the reorganization, China Netcom was fully incorporated into China Unicom in October 2008, reportedly completing the biggest merger in Chinese history.[48] In January 2009, the MIIT issued three 3G licenses, with China Unicom and China Telecom receiving licenses for established 3G services and China Mobile authorized to carry a Chinese TD-SCDMA service, so far unproven, that has been a priority of research and development for the government.[49]

By sheer scope and range of topics—from online novels to video satires[50]—the Internet "cannot be ignored as a battleground for spreading public opinion" and sentiment.[51] Frequently, incidents that go viral (gaining widespread popularity by virtue of being shared on the Internet), are then catapulted into national prominence. These online phenomena also frequently lead to calls for government action and response. According to journalism professor Hu Yong, dedicated coverage by online portals, extensive commentary on discussion forms, and the potency of Internet rumors that reverberate back into

traditional media are driving convergence in the communications industry—especially in spawning "new media events" that often result in consequences for the officials, businesspeople, or celebrities involved.[52] In an unpublished investigative report obtained by David Bandurski of the China Media Project, the vice president of People's Daily Online said that of the secret internal reports sent up to the Central Party Committee each year, two-thirds of the few hundred reports given priority and action by top leaders are from the Internet Office of the State Council Information Office.[53]

The rising prominence of collective efforts over the Internet to target and expose personal data,[54] known as "human flesh search engines," appear to serve a voracious appetite within the Chinese online community for personal accountability. According to Xinhua, the phenomenon had its origins in 2001, when a man posted a picture of a woman he claimed to be his girlfriend on the portal Mop.com, and other Internet users identified her as a model for Microsoft, proving him a liar.[55] Human flesh search engines can initiate investigations as straightforward as looking for missing relatives, but sometimes stray into questionable acts of vigilantism involving threats and harassment. In the years since, human flesh search engines have scored a series of successes in identifying corrupt officials who have acted shamefully or abused their office (and are often subsequently punished), but they have also attacked private individuals engaging in perceived distasteful behavior.[56] They are capable of launching campaigns against people like Grace Wang, a Chinese student at Duke University who was filmed in April 2008 attempting to referee between two opposing groups of protesters at a "Free

Tibet" action on campus.[57] After the video was posted on YouTube and other Web sites, the online reaction was swift: she was lambasted in Chinese-language discussion forums and portals for being "brainwashed" and a "race traitor," among other things, and her parents living in China went into hiding after threats were painted on their apartment.[58]

At times, online activity has tested this relationship between citizens and government on a range of sensitive issues. Signed by over 300 Chinese activists, scholars, lawyers, and others, Charter 08 was issued online on December 9, 2008 as a manifesto inspired by the founding of Charter 77 in Czechoslovakia in 1977.[59] It called for the protection of human rights, an independent judiciary, a republican system of "one person, one vote," and other comprehensive reforms.[60] Charter 08 provoked a clear response from authorities, who questioned or detained more than one hundred of the original signatories, including Liu Xiaobo, a well-known dissident who was detained without process on December 8 and continues (as of May 13, 2009) to be held at an unknown location.[61] However, through circulation by e-mail and other means, Charter 08 had garnered more than 7,000 signatures as of early 2009.[62]

Beyond the hot-button incidents that carry news cycles,[63] the interaction between top-down media supervisory structures and a more porous and unpredictable online sphere have also contributed to the rise of a number of phenomena unique to the Chinese cybersphere. The so-called Fifty Cent Party, a term referring to an estimated 280,000 web commentators nationwide who zealously support the CCP and were initially rumored to net 50 cents per post, are directly organized by the

government to "guide" online public opinion.[64] It had its origins at Nanjing University in 2005, where students were recruited with work-study funds to advocate the Party line on an online student forum, and has been institutionalized to the extent that the Ministry of Culture developed Web commentator trainings (complete with exams and job certification) and major Web sites are required to have in-house teams of these government-trained commentators.[65] Thus, while the government continues to aggressively intervene in news media coverage, these Fifty Cent Party members are proliferating because the Party has also come to recognize the potential benefits of a public relations approach to online discourse.

Legal and regulatory frameworks
Although China's constitution formally guarantees freedom of expression and publication,[66] the protection of human rights,[67] legal and administrative regulations ensure that the Chinese Communist Party will be supported in its strategy of strict supervision of all forms of online content. The Internet has been targeted for monitoring since before it was even commercially available,[68] and the government seems intent on keeping regulatory pace with its growth and development.

Underlying all regulation of the Internet is a pantheon of proscribed content. Citizens are prohibited from disseminating between nine and eleven categories of content that appear consistently in most regulations;[69] all can be considered subversive and trigger fines, content removal, and criminal liability.[70] Illegal content, although broadly and vaguely defined, provides a blueprint of topics the government considers sensitive, including: endangering national security and

contradicting officially accepted political theory, conducting activities in the name of an illegal civil organization, or inciting illegal assemblies or gatherings that disturb social order.[71]

Campaigns directed at cracking down on the perceived harmful societal effects of Internet development have been both publicly mobilized and opaquely implemented, but the latter are no less of a reality. The severity of Internet content control also fluctuates during different time periods, especially those buffering politically sensitive events. For example, an official announcement from the General Administration of Press and Publications that, "a healthy and harmonious environment for a successful 17th Party Congress" would be encouraged by stamping out "illegal news coverage" and "false news," precipitated a crackdown on political news reporting, commentary, and Internet discussion through the close of the Party Congress in October.[72] In those sensitive months, authorities closed 18,401 "illegal" Web sites and targeted Internet data centers, the physical computers that private firms rent to offer online interactive features.[73]

On January 5, 2009, seven ministries (including the Ministry of Public Security and the Ministry of Culture) were convened by the State Council Information Office (SCIO) to discuss selected activities for repairing the flood of "vulgar" (*disu*) content on the Internet that harms the minds and bodies of youth.[74] The crackdown was soon extended to include cell phone messages, online games and novels, videos and radio programs; by January 23, China Internet Illegal Information Reporting Centre (CIIRC) had received nearly 19,000 reports of harmful content, leading authorities to shut down 1,250 illegal Web sites and to delete more

than three million items.[75] The targeting of vulgar and pornographic content also netted some political casualties, notably the blog service provider Bullog.cn (*Niubo*), founded in 2006 by blogger Luo Yonghao. Bullog, which had become an important platform for liberal-leaning intellectuals and political bloggers, was shut down on January 9, 2009 for "picking up harmful information on political and current affairs."[76] Its closure was linked to its status as the leading domestic circulator Charter 08,[77] as it had already survived a suspension in October 2007 during the 17th Communist Party Congress, and the purging of multiple high profile blogs.[78] By April 2009, Luo had migrated the site as Bulloger.com to a server overseas, which was accessible only by proxy server and "unlikely ever to be allowed to exist in China."[79]

In addition to campaigns dedicated to "strict supervision" of online providers in order to curb various types of "harmful" information,[80] the government has managed to develop a relatively comprehensive strategy for managing online media. Since 2004, when essays and articles posted online began to be restricted more systematically, government supervision has evolved to rely largely on informal controls within official structures and stringent formal regulation. Nevertheless, it has been a challenge for the Chinese government to establish the same level of control over the Internet and online media as it has over the traditional media, due to factors including the relative decentralization of government supervision, the scale and viral possibilities of content available online, and the greater number of non-state actors.

A major development in Chinese cyberspace since 2005 has been the flourishing of online news media, which now ranks among the top online activities and reached 234 million Internet users in 2008.[81] Not only do Chinese users cite the Internet as their most important source for information, more important than television and newspapers, but the national information clearinghouse on information technology, the China Internet Network Information Center, acknowledges that "the report[ing] of major events, such as the Olympics, has enabled network[ed] media to stand on a par with mainstream media."[82] Supervision of the media, previously executed primarily by the Propaganda Department of the CCP, has been split with the SCIO, whose local branches have supervisory responsibility over Internet content.[83] For example, most major online content providers and portals are registered in Beijing, and thus are managed by the Beijing Internet Information Administration Bureau under the Beijing Information Office. Web sites and content providers have been reported to operate with greater or lesser levels of freedom depending on where they are registered.[84]

Any organization transmitting content electronically about current politics, economic issues and other public affairs must abide by the 2005 *Provisions on the Administration of Internet News Information Services* (Internet News regulations).[85] These regulations introduced a complex regulatory scheme with the result that only news originating from state-supervised news outlets could be posted online. Government-licensed and authorized news agencies are limited to covering specific subjects approved by the state,[86] but at least are allowed to conduct original reporting on "current events news information," defined as "reporting and commentary relating to

politics, economics, military affairs, foreign affairs, and social and public affairs, as well as reporting and commentary relating to fast-breaking social events."[87] All Web sites that are non-governmental entities, or otherwise not licensed news agencies, are restricted from performing any journalistic function, limiting them to reprinting content from central news outlets or media under the direct control of provincial governments.[88] In practice, major portals are not permitted to repost many articles published by print media online.

To discipline media, government ministries and Party organs use both formal controls, such as policies and instructions and defamation liability, and informal mechanisms, including editorial responsibility for content, economic incentives, intimidation, and other forms of pressure.[89] Generally, authorities prefer to issue instructions advising on topics to be censored informally via SMS, chat, e-mail or at regular meetings with editors. Coverage of politically sensitive events is zealously managed at every stage in order to reduce the risk of exposure to the smallest possible degree.[90] This management includes prior bans on publication and time limits for obeying instructions, as well as "guidance" that serves a more propagandistic function, including instructions on whether to place news, when to place news, where to place it, and in what form it should be publicized. When "mass incidents" or major events such as the 2008 Olympic Games reach their conclusion, the grasp loosens over time, but remains an unrelenting presence.

Despite the challenges and intense resources required to effectively police online media, many of these formal and informal controls have nevertheless been extended to Chinese cyberspace. China's

legal framework for Internet access and usage is achieved by the participation of state and non-state actors at all institutional levels.[91] Control over Internet expression and content is multilayered and achieved by 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. Some of these blunt and frequently applied methods include job dismissals; the closure of Web sites, often by their Web hosting service, for a broad array of infractions;[92] and the detention of journalists, writers, and activists. In 2008, forty-nine individuals were known to be imprisoned for online activities,[93] including several (such as Huang Qi and Du Daobin) serving their second period of detention for Internet-related crimes.[94] Internet users have also been targeted for posting photographs and other multimedia online.[95] For example, journalist Qi Chonghuai was questioned by police about an article he co-wrote about a corrupt local official and photographs of a luxurious government office building on the anti-corruption online forum of the Xinhua News Agency, before being sentenced to four years imprisonment on fraud and extortion charges.[96] Schoolteacher Liu Shaokun was detained on June 25, 2008 and sentenced to one year reeducation-through-labor for posting pictures of school buildings that collapsed in the Sichuan earthquake online.[97]

ICPs, such as BBS and other user-generated content sites, are directly responsible for what is published on their service.[98] All services providing Internet users with information that fail sufficiently to monitor their Web sites and report violations, or produce, publish, or distribute harmful information, face fines

and other serious consequences, including shutdown, criminal liability, and license revocation.[99] The government has used this approach to bring social media like video sharing sites in line with the larger governing framework for Internet content regulation. The *Provisions on the Management of Internet Audio and Video Programming Services* ("Video Regulations"), effective January 1, 2008, were a further refinement of the government's attempt to create a sustainable "walled garden" of self-policed local-language content for the Chinese cybersphere.[100] Jointly issued by the broadcast media regulator State Administration of Radio, Film, and Television (SARFT) and the MIIT, the regulations require video service providers that produce their own content to obtain both a broadcast production license as well as rarely-issued Internet news information services licenses regulated by the MIIT.[101] Correspondingly, video sites are also prohibited from allowing any individuals to upload content pertaining to "current events" news without a special license.[102]

In addition to the types of illegal content routinely proscribed in Internet regulations, SARFT issued a notice on March 30, 2009 detailing twenty-one unusually specific and wide-ranging additional content categories that online video providers should edit or delete.[103] These include distortions of Chinese culture and history; disparaging depictions of revolutionary leaders, heroes, police, army or judiciary; depictions of torture; mocking depictions of catastrophe, including major natural disasters; excessively frightening images and sounds effects; and "sexually suggestive or provocative content that leads to sexual thoughts."[104] The notice also mandates providers to improve their content administration systems by hiring

personnel to review and filter content, especially online music videos and other video entertainment, original content, and even netizen reporters (*paike*).[105]

For the first time, individuals are singled out in the Video Regulations, so that "primary investors" and "managers" can be fined up to 20,000 RMB or barred from engaging in similar services for five years for violations such as not sufficiently policing content or changing shareholders without going through specified procedures.[106]

Implementation of these regulations has been uneven, a trademark of many laws in China. A significant degree of uncertainty was also created by the inaugural requirement that online video service providers be either wholly state-owned (as defined in Article 65 of the 2005 Company Law) or entities where the state holds the controlling interest, until the government clarified in February 2008 that this provision did not apply to already established Web sites.[107] Initially, twenty-five video sharing portals were shut down (including 56.com), and another thirty-two video sharing websites including Tudou.com - China's largest video-sharing portal - were warned for hosting improper material in March 2008.[108] The third-largest Chinese video sharing site, 56.com, went offline mysteriously in June 2008 for more than a month,[109] while Youku.com received a license from SARFT in July 2008.[110]

Technical filtering associated with the so-called Great Firewall of China is only one tool of informal control applied in China. For example, to manage the explosion of the Chinese blogosphere, which reached 162 million blogs at the end of 2008,[111] blog service providers must not only install filters that do not allow the posting of

potentially thousands of keyword combinations, but also flag certain posts for review. Comment sections, forums, and other interactive features that pose a higher risk of containing sensitive content can be shut off, while posts can be deleted or concealed by the provider so that only the author can see them.[112] Bloggers who are considered to have written too many troublesome posts can have their accounts cancelled at will.

The unfolding of one mass incident presents a crucial case study on the range of online and media strategies to gather and communicate information, as well as government attempts to manage them. On June 22, 2008, the body of middle school student Li Shufen was found in the Ximen River in Weng'an county, Guizhou province.[113] Although authorities declared her death to be caused by accidental drowning, her family believed that she was a victim of a crime and pressed for an investigation. Rumors circulated that relatives of the country Party secretary and police chief were among the people Li was with on the night of her death, one of whom said she jumped suddenly while he was doing pushups.[114] Less than a week later, a group of hundreds of marchers heading towards government offices morphed into a crowd of up to 30,000 rioters, who surrounded a police headquarters and set fire to buildings and police vehicles.[115] For a week, local officials were silent and only one piece of news was released by the official Xinhua News Agency, describing protesters as "some people who did not know about the exact context of what had happened."[116] In contrast to the silence of state-run media, numerous photos and video clips of the rioting appeared immediately on blogs and various online forums such as Tianya and the People's Daily Strong China forum, while unconfirmed and

conflicting stories about the girl's death were circulated on the Internet.[117] Angry netizens and Web site moderators dueled vigorously, with users posting in increasingly oblique and creative ways and Web sites aggressively deleting and blocking information about the incident.[118] Furthermore, although hundreds of video clips appeared on YouTube, Chinese users could not access certain videos about the incident, while none appeared on two of biggest China's domestic video sharing sites, Tudou.com and Uume.com.[119] Soon after, state-run media began reporting more news and official announcements regarding the Weng'an riot on Chinese news sites, but without allowing Internet users to leave comments. Other media attempting to cover the story were compelled to apply for special press passes in order to secure interviews, which were then attended by local officials.[120] By early July, state media was providing updates on the girl's cause of death and confirming that four officials had been fired as a result of the incident.[121]

At the same time, because these compulsory control mechanisms are actually implemented through informal processes, provider-based content control is neither narrow nor entirely predictable. A study of Chinese blog service providers demonstrated that there is substantial variation in censorship methods, the amount of content censored, and providers' transparency about deleting or de-publishing content.[122] Similar findings were reached in a Citizen Lab study of four popular search engines in China, which found significant variations in the level of transparency about filtering, actual content censored, and methods used, suggesting that there is not a comprehensive system for determining censored content.[123] While Google and

Microsoft, which are hosted outside China, actually de-listed certain search results, the two search engines hosted inside China, Yahoo! and Baidu, ran their Web crawlers behind the China's filtering system, and therefore did not index Web sites already blocked by the Chinese government. Although Google censored considerably less that the other search engines, it also has a practice of prioritizing authorized local content, which researcher Nart Villeneuve found amplified the significance of the censored Web sites as they were the only ones to offer differing viewpoints.[124] Indeed, the complexity of these informal control mechanisms was further revealed in April 2009, when an employee of China's leading search engine, Baidu.com, leaked a folder containing the substance and flow of internal censorship.[125] These included lists of topics, keywords, and URLs to be blocked, and banned forums, as well as guidelines for employee monitoring work, censorship of the popular Baidu post bars, and information that should be banned.[126]

The government's filtering practices can cause considerable anger amongst China's Internet users, especially when entire platforms or tools such as RSS feed sites or Twitter are blocked. [127] The uses of social media form the building blocks for what blogger Isaac Mao calls "sharism," where the 'co-computing of people, networks, and machines" form a networked pipeline system to spread information in the face of Internet crackdowns.[128]

Due to a wide range of factors – from economic incentives and demographic factors of the online community to the dragnet of legal liability – the impact of self-censorship is likely enormous and increasingly public, if difficult to measure. Furthermore, the efforts of industry

organizations at self-discipline are not entirely removed from government oversight. In promoting "Internet cooperation," officials place self-discipline hand-in-hand with admonitions to abide by Chinese laws.[129] The CIIRC encourages the reporting of "illegal" or "harmful" information and is sponsored by the Internet Society of China, formally registered as a civil society organization.[130] Yet, the CIIRC cited Baidu and Google's Web and image search engines for returning a large number of obscene and pornographic links as part of an announced official crackdown on obscene and pornographic content in January 2009. Google and Baidu were among a total of nineteen Web sites singled out for harmful, vulgar content available to minors, including, Sina.com, Sohu.com, Wangyi, and Tianya.[131]

The Chinese constitution protects people's right to criticize and make suggestions to any state organ.[132] However, a few cases of alleged online defamation publicized in spring 2009 exemplify how the Internet is illuminating some of the complexities of influence and power in the relationships between media, different levels of government, and citizens seeking justice.

Land requisitions for commercial development by local governments in China, where farmers are often inadequately compensated for land and suffer significant losses in income, are a common problem of poor governance and an inadequate legal system.[133] After petitions and other attempts to protect concerned farmers' legal rights had failed, Wu Baoquan and Wang Shuai were detained for their online criticism of local government land seizures.[134] In 2007, Wu had posted information and conducted his own investigation about a land requisition in Ordos, Inner Mongolia, where officials

forced residents off their land in order to sell it to developers. In these land requisitions, they earned exorbitant profits while paying compensation well below market rates to the farmers.[135] Wu was tried twice for criminal defamation and ultimately had his sentence increased to two years, although the same court that affirmed his conviction decided to review his case in April 2009.[136]

Wang Shuai was the author of a satirical blog post suggesting officials from his hometown, Lingbao City in Henan Province, had misappropriated funds for combatting drought by carrying out policies that actually encouraged drought in order to drive down land values and justify paying farmers less compensation for land requisitions.[137] He was detained in Shanghai by Lingbao officials on March 6, 2009, and released on bail only after he signed a written confession and his family agreed to cut down their fruit trees, reducing the compensation they would receive for their land.[138] As is often the case, it took media attention, this time through a story in the national China Youth Daily newspaper, to spark the online public scrutiny that would influence the outcome of Wu's case. In this instance, higher Party officials issued an apology (from the Henan province chief of public security), compensated Wang for his eight days in detention, and fired the local Party secretary and punished three other officials.[139]

Neither Wang nor Wu were journalists using a professional platform to disseminate information, but media were in large part responsible for exponentially expanding public awareness and discourse online on their cases.

The first litigation to be launched over human flesh search engines also tested how Internet libel would be dealt with under Chinese law. A Beijing woman named Jiang Yan had committed suicide in December 2007, months after learning about her husband Wang Fei's infidelity.[140] According to her instructions, posts from the blog diary she left recounting her ordeal were published posthumously by major Web portals, and Wang's anonymous human flesh search engine critics went to work publishing her husband's name, address, and other personal details.[141] In March 2008, after he was publicly condemned, harassed, and fired from his job, Wang sued the classmate of his wife who had posted her blog on his Web site and the portals Daqi.com and Tianya. In December, after convening a rare panel of fifty-four judges, a Beijing court ruled in Wang's favor, finding that the classmate and Daqi.com violated Wang's rights of privacy and reputation, ordering them to pay a total of almost USD1200 in damages for emotional distress, remove the posts, and apologize.[142] However, since Wang admitted to his infidelity, the court did not find that Wang had been slandered. It also exonerated Tianya, which had acted "appropriately" by deleting a user post containing Wang's personal information upon his request.[143] Interestingly, after issuing its judgment the Beijing district court held a press conference to recommend that the MIIT use technology to monitor Internet speech and prevent similar infringements.[144]

While one legal scholar argued that the Chinese legal system "weighs privacy pretty heavily against free speech, even when the speech is truthful,"[145] the relatively low fine may not act as quite as strong a deterrent as plaintiffs like Wang may desire. However, the legal system has become increasingly responsive to those who feel victimized by the human flesh

search engines, especially corrupt officials. In March 2009, the Standing Committee of the National People's Congress approved an amendment to the Criminal Law that would punish government and corporate employees with access to personal data to illegally obtain, sell or leak such information, while Xuzhou city in Jiangsu province became the first jurisdiction to prohibit the dissemination of others' personal information on the Internet.[146]

Surveillance

The government has continued to refine Internet surveillance mechanisms to closely track individuals' online activities.[147] In November 2006 the Ministry of Public Security announced the completion of the essential tasks of constructing the first stage of its "Golden Shield" project, which is a digital national surveillance network with almost complete coverage across public security units nationwide.[148] Despite the vagueness of public pronouncements on the implementation of the Golden Shield, the surveillance efforts of local governments, as well as organizations delegated responsibility for surveillance such as schools and ICPs, are clearly becoming more sophisticated. Since 2006, local governments have been developing "Safe City" surveillance and communications networks that connect police stations, through IP video surveillance, security cameras and back-end data management facilities, to specific locations including Internet cafés, financial centers, and entertainment areas.[149] Private firms known as "censorship entrepreneurs" have also jumped into the fray, providing advanced text mining solutions to enable censors to monitor, forecast and "manage" online public opinion, thereby avoiding scandalous and damaging revelations such as the Internet post in

June 2007 that exposed how children were kidnapped and forced into slave labor at illegal brick kilns in Shanxi province.[150] One company featured by international media, TRS Information Technology, claims to be the "leading search and content management technology and software provider in China," serving over 90 percent of the State Council ministries, 50 percent of newspaper press groups, and 300 universities and colleges.[151] Although TRS disclosed that its high-end surveillance systems had been generally adopted by police – specifically that the company had installed data-mining systems at eight Shanghai police stations so that one Internet police officer could now do the work of ten – TRS does not list the Ministry of Public Security as one of its "famous customers."[152]

Chinese law offers few viable protections for individual privacy, although clauses in most Internet laws and regulations do technically provide for the confidentiality of user information. The exceptions, however, are more important. For example, regulations on the management of e-mail services provide that e-mail service providers are duty-bound to keep personal information and e-mail addresses of users confidential, and may not disclose them except with user consent or when authorized for national security reasons or criminal investigations according to procedures stipulated by law.[153] When required by law, for reasons involving national security and in criminal investigations, most Internet regulations allow for disclosure of user information. However, they typically fail to specify what formal procedures are required or what evidentiary standards must be met for the disclosure of information. In practice, as has been demonstrated in a number of cases,[154] all ISPs and ICPs must not only

capitulate to Chinese government demands for censoring content, but are also required to assist the government in monitoring Internet users and recording their online activities. Requests to turn over personal data are often informal or provide little detail, and providers have no discretion to refuse turning over information to public security officials.[155]

Real-name registration
Registration requirements are often the first step to monitoring citizens' online activities. Although this rule is not enforced, new subscribers to ISPs have been expected to register with their local police bureaus since 1996.[156] In March 2005, as part of a CCP campaign to exercise tighter control over culture, education and media, all university BBS' were ordered to block off-campus users and require users to re-register with their personal identifying information when going online, eliminating online anonymity.[157] The city of Hangzhou was slated to become the first in China to require real-name web registration for users to participate in local chat rooms or online forums, but these regulations were put on hold in May 2009. [158] The momentum for real-name systems might be stronger with cell phones, however. In January 2009, Beijing Mobile announced that it would begin requiring customers to show identification when purchasing its Easyown pre-paid SIM cards (which amount to 70 percent of the customers on China Mobile, the nation's largest carrier) and limit purchases to three per person.[159]

Data retention
ISPs and ICPs in China must fulfill data retention obligations. ISPs are required to record important data (such as identification, URLs visited, length of visit, and activities) about all of their users for

at least sixty days and to ensure that no illegal content is being hosted on their servers.[160] While 78 percent of users in China connect from home, 42 percent of users also use Internet cafés as a main access location.[161] However, since 2002, Internet access through Internet cafés has heavily been regulated: all cafés are required to install filtering software, ban minors from entering, monitor the activities of their users, and record every user's identity and complete session logs for up to sixty days.[162] In many cities, they are also connected by live video feed to local police stations. The providers of electronic bulletin services, including bulletin board services, online discussion forums, chat rooms, *et cetera* are required to monitor the contents of information released in their service system, time of release, URL or domain name, and keep it for sixty days.[163]

Owned by Tencent, QQ is China's most popular instant messenger, and this service was found to have installed a keyword blocking program in their client software to monitor and record users' online communication, offering it to the police if required.[164]

Filtering and surveillance are often complementary processes, especially when ISPs and ICPs that are liable for the activities of their users delegate human monitors to monitor and flag content for further review or deletion. Online communications via e-mail and instant messaging (such as QQ and Skype) are also examined and monitored by government.[165] In October 2008, a joint report by the Information Warfare Monitor and ONI Asia provided a chilling example of the possibilities for surveillance conducted by non-state actors on a massive scale.[166] TOM-Skype, the Chinese-marketed version of the chat and

texting software Skype, kept over a million user records in seven types of log files, including IP addresses, usernames, and time and date stamps in all the log files that could be decrypted. All of these log files, along with the information required to decrypt these log files, were kept on publicly-accessible servers. For call information logs dating from August 2007, the username and phone number of the recipient was also logged, while content filter logs dating from August 2008 also contained full texts of chat messages (which themselves contained sensitive information such as e-mail addresses, passwords, and bank card numbers). Of the eight TOM-Skype surveillance servers traced by researcher Nart Villeneuve, one server hosted a special version designed for use in Internet cafés and contained log files and the censored keyword list, while another contained logs for TOM Online's wireless services.

The TOM-Skype surveillance system was triggered when a TOM-Skype user sent or received messages containing a banned keyword listed in a keyfile, and those messages are then stored in log files on a TOM-Skype server. Within the content of these messages stored in the file logs, when filtered out to eliminate English language obscenities, almost 16 percent contain the word 'communist,' 7 percent the word 'falun,' and 2.5 percent contained 'Taiwan independence.' However, the logged messages also made reference to other content outside the range of these long-sensitive topics, such as earthquake and milk powder.[167]

Furthermore, the data also contained personal information of Skype users that interacted with TOM-Skype users. Users who attempt to access www.skype.com from China are redirected to skype.tom.com. While Skype claimed that

TOM fixed the security breaches within twenty-four hours of the report's publication,[168] the report issued a warning for "groups engaging in political activism or promoting the use of censorship circumvention technology accessed through services provided by companies that have compromised on human rights." From the information contained in the log files, it would be possible to conduct politically motivated surveillance by using simple social networking tools to identify the relationships between users.

Like all other ICPs, most bulletin boards and chat rooms assign personnel to monitor the content of messages.[169] Messages submitted by users are censored by human censors and filtering systems before appearing online.[170] In order to enhance the surveillance on bulletin board systems, since 2005, the users of campus bulletin boards have been mandated to re-register with their real identifying information before posting messages online.[171]

In recent years, serious concerns have been raised about the ability of the Chinese government to spy on the country's 624 million cell phone subscribers: in 2008, one Chinese state-run cell phone company revealed that it had unlimited access to the personal data of their customers and hands the date over to Chinese security officials upon request.[172] Since 2004, the Chinese government has been drafting legislation to regulate personal mobile phone communication, which would require all cell phone subscribers to register for mobile phone service with their real name and identification card.[173] In addition, Chinese police have installed filtering and surveillance systems for mobile and short message service providers to block and monitor "harmful" short message

communications.[174] Anyone who distributes "harmful" message or rumors via short message service of mobile phones can be arrested and convicted. [175]

Cyberattacks
In 2008, organizations advocating for human rights in Tibet and China experienced escalated cyberattacks during politically explosive events, such as the crackdown on Tibetan protesters in March, and in the lead-up to the Olympic Games in August. The preferred method of these attackers was reportedly email viruses, which are more likely to be undetected by commercial anti-virus software because they are hand-crafted.[176] From field research conducted at the offices of the Tibetan Government-in-exile in Dharamsala and several Tibetan missions abroad, researchers at the SecDev Group and the Citizen Lab at the University of Toronto discovered an extensive malware based cyber-espionage network that also used "contextually relevant emails" to gain "complete, real-time" control of at least 1,295 infected computers in 103 countries.[177] This network, which they called GhostNet, sent emails to specific targets containing a Trojan called gHost RAT, which in taking full control of infected computers allowed GhostNet to search and download specific files and covertly operate attached devices such as microphones and web cameras. Among the high-value infections, comprising close to 30 percent of the computers affected, were many foreign affairs ministries, embassies, regional organizations (such as the ASEAN Secretariat) and news organizations. Although the complicity or awareness of Chinese authorities could not be conclusively established, researchers tracked the instances of gHost RAT to commercial Internet access accounts located on the island of Hainan in China.

ONI testing results
The 'great firewall of China' uses a variety of overlapping techniques for blocking content containing a wide range of material considered politically sensitive by the Chinese government. While China employs filtering techniques used by many other countries, including DNS (domain name system) tampering and IP (internet protocol) blocking, it is unique in the world for its system of Internet connections when triggered by a list of banned keywords. Known as a TCP reset, this content filtering by keyword targets content regardless of where it is hosted.

TCP reset filtering is based on inspecting the content of IP packets for keywords that would trigger blocking, either in the header or the content of the message. When a router in the Great Firewall identifies a bad keyword, it sends reset packets to both the source and destination IP addresses in the packet, breaking the connection.

China employs targeted yet extensive filtering of information that could have a potential impact on the Party's control over social stability, and is therefore predominantly focused on Chinese-language content relating to China-specific issues. For the government, information constituting a threat to public order extends well beyond well-publicized sensitive topics, such as the June 1989 military crackdown, the Tibetan rights movement, and the Falun Gong spiritual organization (all of which are methodically blocked), and includes independent media and dissenting voices, as well as content on human rights, political reform, sovereignty issues, and circumvention tools.

Filtering during the 2008 Olympic Games

ONI monitored a shortlist of prominent blogs, Chinese-language and international news sites, advocacy organizations, and social media platforms continuously from late July to mid-September 2008. This period generally marked the one of most significant openings in access to information since ONI began monitoring Internet filtering in China in 2004, but the foundations of censorship based on control over domestic media and civil society remained.

In 2001, China issued this decree in its official bid for the 2008 Olympic Games: "There will be no restrictions on journalists in reporting on the Olympic Games."[178] This promise was significantly compromised, not only in China's purported long-term attempt to build a more open and transparent media system,[179] but also in the lack of transparency over its policy on access to online information.

At a press conference on July 28, the media director of the Beijing Olympic Committee responded to a Wall Street Journal reporter who physically displayed the filtering of certain websites on his laptop by denying anything was amiss.[180] This time, a Chinese Foreign Ministry spokesperson laid part of the blame with the websites themselves, claiming they have problems making them "not easy to view in China."[181] Yet three days later, on July 31, the IOC admitted to accepting a deal with the Chinese government in which sensitive websites that were "not considered Games-related" would be blocked.[182]

During the Olympics, access was partitioned between the Olympics Main Press Center (MPC) in the Olympic Green and the Beijing International Media Center, the main press venue for non-IOC accredited journalists.[183] ONI compared data from the MPC and other locations in Beijing, compiling a snapshot of Internet filtering in China leading up to the Olympics. ONI testing confirms that filtering of Internet content at the MPC continued even for members of the foreign press through TCP reset keyword blocking and IP address blocking; the latter accounting for the vast majority of filtering at the MPC. For each test at the MPC, ONI tested at other locations in Beijing with broadband Internet access provided by China Netcom. Throughout this time period, filtering was nearly identical between the MPC and consumer-level access on China Netcom and China Telecom, indicating that the incrementally increased openness was implemented nationally.

Many sites that are routinely blocked by the Chinese government for containing politically sensitive content remained accessible from August 1 to at least mid-September 2008, including the website of human rights organizations (Article 19, China Labour Bulletin) and foreign-hosted Chinese-language news sites. Overseas news organizations such as the World Journal and the BBC News Chinese website were the main beneficiaries of China's Olympic guarantees.

Even though the IOC acknowledged on July 31 that filtering would continue to take place, a number of websites blocked at the MPC on July 25 were accessible a week later, including Amnesty International, Chinese-language Wikipedia (zh.wikipedia.org), and an increased swath of independent media including Taiwan's Liberty Times, the Hong Kong-based Apple Daily newspaper, Voice of America news, and Radio Free Asia (www.rfa.org) and its Chinese website.

However, RFA's Tibetan and Uyghur language websites became inaccessible again around August 20. Although Flickr remained accessible throughout the testing period, two of its photo servers were filtered until mid-August. Most of the sites unblocked for the Olympics remained accessible until at least mid-September 2008 on China Netcom, although a few (including Amnesty International) were again blocked on China Telecom by September 15.

At the same time, ONI found that the sites being filtered frequently address tumultuous and controversial changes wrought in preparation for the Games, from crackdowns on civil society to the transformation of a capital city and other social upheavals. Thus, the majority of advocacy sites and politically 'sensitive' organizations remained blocked, sweeping across a broad range of issues from citizen journalism (www.zuola.com) to the Three Gorges Probe, as well as nearly all of the Tibetan exile advocacy groups. Groups staunchly critical of Chinese government policy, including the press freedom groups Reporters Without Borders and Freedom House, continued to be blocked. The status of certain news sites including the China Digital Times Internet news and information clearinghouse, and Boxun.com, a dissident news website that Chinese government officials reportedly look to as a source of internal news, remained unchanged. Furthermore, the accessibility of any website does not guarantee that content on that site will be available, as China's practice of filtering keywords through a TCP reset appears as robust as ever.

On December 19, 2008, the website of The New York Times was reported blocked even as restrictions were lifted on the

Chinese-language Web sites of the BBC, Voice of America and Asiaweek, which had been blocked earlier that week. [184]

In addition to testing during the Olympics period, ONI also conducted testing in late 2008 on two backbone providers, the state-owned telecoms China Unicom, (CU), formerly China Netcom, and China Telecom (CT), which between them provide coverage nationwide. Because both control access to an international gateway, URL filtering and domain name system (DNS) tampering implemented by CU and CT affect all users of the network regardless of ISP.

Nearly all of the DNS tampering was executed by CU, while CT blocked a number of human rights organizations, pornographic sites, and one Hong Kong-based publisher (mirrorbooks.com) using this method. CU also uses IP blocking to filter nearly 400 IP addresses. These correlated closely to sites blocked on CT through a method obscured to analysis, in which users were presented with an error page informing the user that a network error occurred while accessing the website. While the error page can appear in the case of legitimate network errors, the repeated appearance of the error page indicates blocking is taking place. CT also used a squid proxy to block a handful of websites, including several Flickr photo servers. While the two backbone providers showed less overlap in filtering methods when compared with 2006-2007, there continues to be almost complete correlation in blocking between CU and CT.

At time of testing, most international social media platforms were accessible, including Flickr, Blogspot, Wordpress, Facebook, and Twitter. In contrast to 2006-2007, when all individual Blogspot

blogs tested were accessible on China Netcom and blocked or inaccessible on China Telecom, in 2008 CU and CT blocked nearly all of the same individual Blogspot blogs tested. Technorati continued to be blocked.

In late 2008, China had resumed blocking many Web sites that were blocked in 2006-2007 and made accessible during at least part of the Olympics period. These included the independent overseas news sites (The Liberty Times) and Radio Free Asia's main website and its Mandarin, Uyghur, and Tibetan language sites. However, in contrast to 2006-2007, some of these websites were unreliably or intermittently accessible during December 2008 testing, possibly as a result of the TCP reset filtering method used. Sites blocked using the TCP reset included YouTube, Chinese-language Wikipedia, and BBC News.

A few sites that were accessible in 2006-2007 had been blocked by the time of testing in 2008, most notably Wikipedia, (en.wikipedia.org). The site Wikileaks was also blocked by both ISPs in 2008 testing.

The greatest variations in filtering patterns between 2006-2007 and 2008 occurred with Chinese-language news media Web sites, likely in continuity from the Olympics. As in 2006-2007, few international news organizations were filtered, and some formerly blocked (e.g. Voice of America News) were accessible. Notably, some prominent Chinese-language media blocked in 2006-2007 were accessible in 2008, including the World Journal, www.singtao.com, and the Apple Daily. However, a significant number of independent media representing different points on the political spectrum continued to be filtered.

In 2006-2007 and 2008, China filtered a significant portion of content specific to its own human rights record and practices. As such, only a few global human rights sites with a global scope continued to be filtered, including Human Rights and Freedom House. Article 19 and Human Rights First were no longer blocked in 2008, and filtering on Amnesty International was renewed after a hiatus during the Olympics period. A typical example of this targeting of China-related content is the differential treatment of two related organizations: while the Web site for the writers' association PEN American Center hosted content on the jailed dissident and Charter 08 co-author Liu Xiaobo, it was accessible (www.pen.org) while the Chinese PEN Center (www.chinesepen.org), a site with both English and Chinese content, was blocked by both ISPs. The sites of watchdogs on Chinese rights defenders and labor rights continued to be blocked, as did a substantial number of rights organizations based in Hong Kong.

Certain targets for blocking continued to cut across political and social lines of conflict in 2008. The consistent filtering of Web sites supporting greater autonomy and rights protection for the Uyghur (http://www.uyghurcongress.org/), Tibetan, and Mongolian (http://www.innermongolia.org/) ethnic minorities is not surprising, as these issues have already been excluded from official discourse inside China. Nearly all of the overseas Tibetan organizations, which conduct a wide range of activities from news broadcasting for the Tibetan community to the Tibetan Youth Congress, which lobbies for full independence for Tibet. China also continued to block a substantial number of sites on religion, including the International Coalition for Religious Freedom, Catholic organizations,

and sites on Islam in Arabic, including those presenting extremist viewpoints (http://www.alumah.com/).

In 2008, China continued to filter a significant number of sites presenting alternative or additional perspectives on its policies toward Taiwan and North Korea. For example, the Democratic Progressive Party (DPP) of Taiwan (http://www.dpp.org.tw/) is continually filtered. However, a number of sites with no political content but ending with the domain .tw were blocked, and Greenpeace Taiwan was the only country website of the organization blocked by both ISPs.

As in 2006-2007, the major exceptions to the focus on politically sensitive topics specific to China in 2008 were circumvention tools and pornography. A portion, though not a majority, of proxy tools and anonymizers in both the Chinese (http://gardennetworks.com/) and English languages (http://www.peacefire.org/) was blocked. The circumvention tool Psiphon is also blocked, along with the Citizen Lab at the University of Toronto and the Information Warfare Monitor, sister institutions engaging in research on circumvention and surveillance. Both ISPs also blocked a substantial amount of pornographic content.

Although the scope of Internet filtering in China extends far beyond the highly sensitive issues known as the "three Ts: Tibet, Tiananmen, and Taiwan," the continued potency of these subjects evidently prompted the Chinese government to step up filtering of leading international websites and social media platforms in 2009. On March 24, 2009, Google officially confirmed that YouTube was blocked in China, from a steep drop in traffic on the evening of March 23 to "near zero" by March 24.[185] Herdict.org

also captured accounts providing evidence of a previous reported block of Youtube beginning on March 4, coinciding with the one-year anniversary of the crackdown on protests in Tibetan regions (during which YouTube was also reported blocked in March 2008) as well as the 50th anniversary of the Tibetan uprising of 1959. Blogspot became inaccessible around May 9,[186] and on June 2, two days before the 20th anniversary of the June 4th military crackdown, Flickr, Twitter, live.com, and Hotmail were blocked in rapid succession.[187]

In May 2009, the Ministry of Industry and Information Technology (MIIT) in China sent a notification to computer manufacturers of its intention to require all new PCs sold in China after July 1 to have filtering software pre-installed.[188] The notice, jointly issued by the MIIT, the Civilization Office of the Central Communist Party Committee, and the Ministry of Finance, according to the PRC Government Procurement Law, mandates the procurement of all rights and services related to a designated software called "Green Dam Youth Escort" to be made available for free public use in accordance with the Government Procurement Law. Green Dam is a product of the Jinhui Computer System Engineering Co., which reportedly received 40 million RMB from the government for a year-long contract.[189]

The purported intent of the Green Dam software is to filter harmful online text and image content in order to prevent the effects of this information on youth and promote a healthy and harmonious Internet environment.[190] However, researchers at the OpenNet Initiative and the Stop Badware project conducting an initial technical assessment of the software found that Green Dam's filtering

is not only ineffective at blocking pornographic content as a whole, but also includes unpredictable and disruptive blocking of political and religious content normally associated with the Great Firewall of China.[191]

As a computing tool Green Dam is far more powerful than the centralized filtering system China currently implements. It actively monitors individual computer behavior to the extent that its 'language processing' tool can institute extremely intrusive 'kill' action on sites if the content algorithm detects 'inappropriate' sensitive political or religious speech.[192] These actions include the sudden termination of web browser tabs, whole browsers, and a wide range of programs including word processing and email. In order to enable this application layer monitoring, Green Dam installs components deep into the kernel of the computer operating systems. Researchers also found that the killing of sites upon inappropriate keywords or URLs like "falundafa.org" extends to killing single letters that auto-complete in the location boxes and auto-complete lists in browsers. For example, if a user enters epochtimes.com into the location, the user will see the page briefly, see the warning box briefly, and then have the whole browser killed. But after the user restarts the browser, epochtimes.com will be in the browser history and therefore in the auto-complete list, so that the user may only have to type 'e' into the location box to trigger the appearance of epochtimes.com in the auto-complete list and cause Green Dam to kill the whole browser.[193]

The monopoly status granted to Jinhui is unprecedented, representing the first instance where a government mandated a specific filtering software product for use at a national level instead of performance standards that encourage consumer choice, security and product quality. The mandated procurement and pre-installation of Green Dam also adds a new and powerful control mechanism to the existing filtering system, in addition blocking already done at the international backbones and by individual online content providers. Distributing control mechanisms to end-users at the periphery allows the government to partially offload the burden of monitoring and blocking content to individual machines on the network, amounting to a "huge distributed super computer dedicated to controlling online content."[194]

In addition to interfering with the performance of personal computers in an unpredictable way, the poor design of Green Dam also presents security risks that allow any web site the user visits to take control of the user's computer, with the potential for malicious sites to steal private data and other illegal acts, or even turn every Chinese computer running Green Dam into a member of a botnet.[195] The StopBadware Project at the Berkman Center confirmed that the application violates its Badware guidelines for software, as it does not disclose the filtering of political speech or the unexpected behavior of completely killing processes that contain such speech.[196]

Conclusion
In 2008, China led the world with 300 million Internet users, and the sheer scale and expanding scope of online content presented a significant challenge for a government intent on maintaining social stability and order in China's networked spheres. The 2008 Olympic Games held in Beijing had a net positive impact on access to information, but this has abated without continued international pressure for greater openness and transparency.

The foundation of China's information control framework continues to be built on ensuring domestic providers are responsible for filtering and monitoring hosted content. In fine-tuning this system China is also adopting subtler and more fluid controls, including attempts to promote a public relations approach to online commentary and news reporting as well as measures to distribute control mechanisms to end users through the procurement of filtering software on home computers.

NOTES

1 Jim Yardley, "Monk Protests in Tibet Draw Chinese Security," March 14, 2008, http://www.nytimes.com/2008/03/14/world/asia/14china.html.

2 Jim Yardley, "Tibetans Clash With Chinese Police in Second City," March 16, 2008, http://www.nytimes.com/2008/03/16/world/asia/16tibet.html?ref=asia.

3 Roland Soong, "The Olympic Torch Tour As Public Relations Disaster," EastSouthWestNorth blog, April 10, 2008, http://zonaeuropa.com/20080410_1.htm.

4 Dune Lawrence and Lee Spears, "China Rejects CNN Apology, Demands 'Sincere' Response," Bloomberg, April 16, 2008, http://www.bloomberg.com/apps/news?pid=20601204&sid=aVlfJJeTKWMc; Xinhua News Agency, "Chinese netizens urge Carrefour boycott after torch relay incident," April 16, 2008, http://news.xinhuanet.com/english/2008-04/16/content_7989807.htm.

5 BBC News, "China earthquake toll jumps again," May 23, 2008, http://news.bbc.co.uk/2/hi/asia-pacific/7416035.stm.

6 Qian Gang, "Looking back on Chinese media reporting of school collapses," China Media Project, May 7, 2009, http://cmp.hku.hk/2009/05/07/1599/; Edward Wong, "Year After China Quake, New Births, Old Wounds," May 6, 2009, http://www.nytimes.com/2009/05/06/world/asia/06quake.html.

7 Tania Branigan, "China releases earthquake death toll of children," The Guardian (UK), May 7, 2009, http://www.guardian.co.uk/world/2009/may/07/china-earthquake-anniversary-death-toll.

8 Qian Gang, "Looking back on Chinese media reporting of school collapses," China Media Project, May 7, 2009, http://cmp.hku.hk/2009/05/07/1599/.

9 Michael Bristow, "Big Olympic spend, but little debate," BBC News, July 31, 2008, http://news.bbc.co.uk/2/hi/asia-pacific/7523235.stm.

10 REGULATIONS ON REPORTING ACTIVITIES IN CHINA BY FOREIGN JOURNALISTS DURING THE BEIJING OLYMPIC GAMES AND THE PREPARATORY PERIOD, issued January 8, 2007, http://www.chinese-embassy.org.uk/eng/lsyw/Journalist/t287657.htm.

11 Jacquelin Magnay, "China's media censored over stabbing," The Age, August 12, 2008, http://www.theage.com.au/world/chinas-media-censored-over-stabbing-20080811-3tmf.html.

12 OpenNet Iniative blog, "The Catch-22 of protests and surveillance," August 19, 2008, http://opennet.net/blog/2008/08/the-catch-22-protests-and-surveillance.

13 Foreign Correspondents' Club of China, "Reporting Interference Tally Update," http://www.fccchina.org/2008/12/03/reporting-interference-tally-update/; Foreign Correspondents' Club of China Statement, "China Fails To Make Olympic Podium On Media Freedom," August 23, 2008, http://www.fccchina.org/2008/08/23/china-fails-to-make-olympic-podium-on-media-freedom/#more-35.

14 BBC News, "China's press freedoms extended," October 18, 2008, http://news.bbc.co.uk/2/hi/asia-pacific/7675306.stm.

15 Foreign Correspondents' Club of China, "FCCC Urges Withdrawal Of Restrictions On HK Journalists," February 13, 2009, http://www.fccchina.org/2009/02/13/fccc-urges-withdrawal-of-restrictions-on-hk-journalists/.

16 Xinhua News Agency, "60 arrested over melamine-tainted Sanlu milk powder," January 11, 2009, http://www2.chinadaily.com.cn/china/2009-01/11/content_7385532.htm.

17 The Australian, "China accused of Olympic milk cover-up," October 1, 2008, http://www.theaustralian.news.com.au/story/0,25197,24430439-2703,00.html.

18 Jim Yardley and David Barboza, "Despite Warnings, China's Regulators Failed to

Stop Tainted Milk," The New York Times, September 27, 2008, http://www.nytimes.com/2008/09/27/world/asia/27milk.html?pagewanted=print.

[19] Jim Yardley and David Barboza, "Despite Warnings, China's Regulators Failed to Stop Tainted Milk," The New York Times, September 27, 2008, http://www.nytimes.com/2008/09/27/world/asia/27milk.html?pagewanted=print.

[20] Zhu Zhe and Cui Xiaohuo, "Sanlu ex-boss gets life for milk scandal," China Daily, January 22, 2009, http://www.chinadaily.com.cn/china/2009-01/22/content_7422297.htm.

[21] David Bandurski, "Taxi strikes in China highlight changing press controls," China Media Project, November 12, 2008, http://cmp.hku.hk/2008/11/12/1344/.

[22] Tania Branigan, "China tells state media to report bad news," The Guardian (UK), November 20, 2008, http://www.guardian.co.uk/media/2008/nov/20/china-media-freedom.

[23] Maureen Fan, "In China, Media Make Small Strides," The Washington Post, December 28, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/12/27/AR2008122701218.html.

[24] David Bandurski, "The Longnan riots and the CCP's global spin campaign," China Media Project, November 20, 2008, http://cmp.hku.hk/2008/11/20/1368/.

[25] Reuters, "China to introduce journalist 'black list,'" February 13, 2009, http://in.reuters.com/article/worldNews/idINIndia-37996920090213?sp=true.

[26] David Bandurski, "In today's headlines, an absence speaks a thousand words," May 27, 2009, http://cmp.hku.hk/2009/05/27/1647/.

[27] Andrew Jacobs, with Jonathan Ansfield, "Chinese Learn Limits of Online Freedom as the Filter Tightens," The New York Times, February 5, 2009, http://www.nytimes.com/2009/02/05/world/asia/05beijing.html.

[28] Foreign Correspondents' Club of China Statement, "China Should Allow Access To Tibetan Areas," March 9, 2009, http://www.fccchina.org/2009/03/09/china-should-allow-access-to-tibetan-areas/.

[29] China Internet Network Information Center, "Twenty-third Statistical Survey Report on the Internet Development in China," issued March 23, 2009, http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf.

[30] China Internet Network Information Center, "Twenty-third Statistical Survey Report on the Internet Development in China," issued March 23, 2009, http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf.

[31] Bloomberg, "China to Merge Telecom Companies, Issue 3G Licenses", May 24, 2008, http://www.bloomberg.com/apps/news?pid=20601087&sid=an0_Sig7jjE0&refer=home.

[32] China Internet Network Information Center, "Twenty-third Statistical Survey Report on the Internet Development in China," issued March 23, 2009, http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf.

[33] China Internet Network Information Center, "Twenty-third Statistical Survey Report on the Internet Development in China," issued March 23, 2009, http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf.

[34] China Internet Network Information Center, "Twenty-third Statistical Survey Report on the Internet Development in China," issued March 23, 2009, http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf.

[35] Zhao Zhiguo, "Development and Administration of Internet in China," http://www.china.org.cn/china/internetForum/2008-11/06/content_16719106.htm.

[36] China Internet Network Information Center, "Twenty-third Statistical Survey Report on the Internet Development in China," issued March 23, 2009, http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf.

[37] China Internet Network Information Center, "Twenty-third Statistical Survey Report on the Internet Development in China," issued March 23, 2009, http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf.

[38] China Internet Network Information Center, "Twenty-third Statistical Survey Report on the Internet Development in China," issued March 23, 2009, http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf.

[39] Paul Budde Communication Pty Ltd., "China: New Internet Economy," April 24, 2009.

[40] SinoCast China IT Watch, "China to issue its first VoIP license," March 13, 2006.

[41] CC Time, "Analysis of recent developments and forecasts for China's VOIP industry," March 19, 2008, http://www.cctime.com/html/2008-3-19/20083191040597146.htm.

[42] Ministry of Industry and Information Technology of the People's Republic of China, http://www.miit.gov.cn/n11293472/index.html.

[43] People's Daily Online, "Highlights of China's institutional restructuring plan," March 16, 2008, http://english.peopledaily.com.cn/90001/90776/90785/6374104.html.

[44] China Internet Network Information Center, "Twenty-third Statistical Survey Report on the Internet Development in China," issued March 23, 2009, http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf.

[45] China Internet Network Information Center, "Twenty-third Statistical Survey Report on the Internet Development in China," issued March 23, 2009, http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf.

[46] Paul Budde Communication Pty Ltd., "China: Telecommunications Infrastructure," April 24, 2009.

[47] *Ibid.*

[48] Xinhua News Agency, "China Netcom, China Unicom merger completed, biggest in country's history," October 15, 2008, http://news.xinhuanet.com/english/2008-10/15/content_10200183.htm.

[49] Sumner Lemon, "After Years of Delays, China Finally Issues 3G Licenses," IDG News Service, January 7, 2009, http://www.pcworld.com/businesscenter/article/156612/after_years_of_delays_china_finally_issues_3g_licenses.html.

[50] "Where there are River Crabs, there are Grass-Mud Horses" (*nali you hexie, nali you caonima*)" is based on plays on characters and meaning, forming a "law of Chinese cyberpolitics": online censorship always meets resistance. See http://chinadigitaltimes.net/china/grass-mud-horse/.

[51] China Internet Network Information Center, "Twenty-third Statistical Survey Report on the Internet Development in China," issued January 2009 (Chinese), http://www.cnnic.net.cn/uploadfiles/pdf/2009/1/13/92458.pdf.

[52] Alice Xin Liu, "Hu Yong interview: the digital age, Orwell's 'Newspeak' and Chinese media," Danwei, April 16, 2009, http://www.danwei.org/media/hu_yong_interview.php.

[53] David Bandurski, "China's Guerrilla War for the Web," Far Eastern Economic Review, July 2008, http://www.feer.com/essays/2008/august/chinas-guerrilla-war-for-the-web.

[54] Lokman Tsui, "Day 2 4.1: Chen Lu, Human Flesh Search," May 28, 2009, http://www.lokman.org/2009/05/28/day-2-41-chen-lu-human-flesh-search/.

[55] Bai Xu and Ji Shaoting, "'Human flesh search engine': an Internet lynching?", Xinhua News Service, July 4, 2008, http://news.xinhuanet.com/english/2008-07/04/content_8491087.htm.

[56] Ryan McLaughlin, "Human flesh search engines – crowd-sourcing 'justice,'" CNet Asia Blogs: The Tech Dynasty, January 28, 2009, http://asia.cnet.com/blogs/thetechdynasty/post.htm?id=63008617.

57 "Grace Wang," YouTube,
   http://www.youtube.com/watch?v=zomgZ
   uZoDoM.

58 National Public Radio, "Duke Student
   Targeted for Mediating Tibet Protest," April
   21, 2008,
   http://www.npr.org/templates/story/story.
   php?storyId=89803198.

59 Charter 08, Unofficial translation at
   http://www.nybooks.com/articles/22210;
   http://www.hrichina.org/public/contents/
   press?revision_id=89851&item_id=8571
   7.

60 Charter 08, Unofficial translation at
   http://www.nybooks.com/articles/22210;
   http://www.hrichina.org/public/contents/
   press?revision_id=89851&item_id=8571
   7.

61 China Human Rights Defenders, "Over One
   Hundred Signatories Harassed Since
   Launch of Charter 08," January 8, 2009,
   http://crd-
   net.org/Article/Class9/Class98/200901/
   20090108141140_12945.html.

62 John Garnaut, "Late-night visit from police
   as Charter 08 support grows," The Sydney
   Morning Herald, January 13, 2009,
   http://www.smh.com.au/articles/2009/0
   1/12/1231608616941.html.

63 Roland Soong, "A Review Of The Chinese
   Internet In 2008," EastSouthWestNorth
   blog, January 24, 2009,
   http://www.zonaeuropa.com/20090124_
   1.htm.

64 David Bandurski, "China's Guerrilla War for
   the Web," Far Eastern Economic Review,
   July 2008,
   http://www.feer.com/essays/2008/augus
   t/chinas-guerrilla-war-for-the-web.

65 David Bandurski, "China's Guerrilla War for
   the Web," Far Eastern Economic Review,
   July 2008,
   http://www.feer.com/essays/2008/augus
   t/chinas-guerrilla-war-for-the-web.

66 Article 34, Constitution of the People's
   Republic of China, amended March 14,
   2004, by the 10th NPC at its 2nd Session,
   http://english.peopledaily.com.cn/constit
   ution/constitution.html.

67 Article 33, Constitution of the People's
   Republic of China, amended March 14,
   2004, by the 10th NPC at its 2nd Session,
   http://english.peopledaily.com.cn/constit
   ution/constitution.html.

68 See the Regulations of the People's
   Republic of China for the Safety Protection
   of Computer Information Systems
   (*Zhonghua renmin gongheguo jisuanji
   xitong anquan baohu tiaoli*), issued by the
   State Council on February 18, 1994.

69 The nine types of content that have been
   illegal to produce or disseminate since the
   earliest Internet Regulations are: 1)
   violating the basic principles as they are
   confirmed in the Constitution; 2)
   endangering state security, divulging state
   secrets, subverting the national regime, or
   jeopardizing the integrity of national unity;
   3) harming national honor or interests; 4)
   inciting hatred against peoples, racism
   against peoples, or disrupting the
   solidarity of peoples; 5) disrupting national
   policies on religion, propagating evil cults
   and feudal superstitions; 6) spreading
   rumors, disturbing social order, or
   disrupting social stability; 7) spreading
   obscenity, pornography, gambling,
   violence, terror, or abetting the
   commission of a crime; 8) insulting or
   defaming third parties, infringing on legal
   rights and interests of third parties; and 9)
   other content prohibited by law and
   administrative regulations. Two categories
   of prohibited content were added in Article
   19 of the Provisions on the Administration
   of Internet News Information Services
   (Internet News Information Services
   Regulations) (*hulianwang xinwen xinxi
   fuwu guanli guiding*), promulgated by the
   State Council Information Office and the
   Ministry of Information Industry on
   September 25, 2005. These two
   additional categories are 1) inciting illegal
   assemblies, associations, marches,
   demonstrations, or gatherings that disturb
   social order; and 2) conducting activities
   in the name of an illegal civil organization.
   Translation is available at

http://www.cecc.gov/pages/virtualAcad/index.phpd?showsingle=24396.

[70] See, for example, Rules of the NPC Standing Committee on Safeguarding Internet Security (*Quanguo renda changweihui guanyu weihu hulianwang anquan de guiding),* issued by the NPC Standing Committee on December 28, 2000.

[71] Article 19, *Provisions on the Administration of News Information Services,* issued by the Ministry of Information Industry and the State Council Information Office on September 25, 2005, http://www.isc.org.cn/20020417/ca315779.htm (Chinese), unofficial English translation at http://www.cecc.gov/pages/virtualAcad/index.phpd?showsingle=24396.

[72] Human Rights Watch Press Release, "China: Media Chokehold Tightens Before Party Congress," August 17, 2007, http://china.hrw.org/press/news_release/china_media_chokehold_tightens_before_party_congress. See also Michael Bristow, "China tightens grip ahead of congress," BBC News, September 14, 2007, http://news.bbc.co.uk/2/hi/asia-pacific/6992946.stm.

[73] Peter Ford, "Why China shut down 18,401 websites," Christian Science Monitor, September 25, 2007, http://www.csmonitor.com/2007/0925/p01s06-woap.html?page=1.

[74] Xinhua News Agency, "Seven departments launch operation for fixing the spread of vulgarity on the Internet," (*qi bumen kaizhan zhengzhi hulianwang disu zhifeng xingdong*), January 5, 2009, http://www.gov.cn/jrzg/2009-01/05/content_1196447.htm.

[75] Xinhua News Agency, "Porn crackdown to shield China's youth during holiday," China.org.cn, January 23, 2008, http://www.china.org.cn/china/news/2009-01/23/content_17178010.htm.

[76] Vivian Wu, "Popular Blog Service Provider Shut Down," South China Morning Post, January 10, 2009.

[77] John Garnaut, "Nervous China tightens grip on internet," Sydney Morning Herald, January 12, 2009.

[78] China Digital Times, "Bullog shut down," January 9, 2009, http://chinadigitaltimes.net/2009/01/bullog-shut-down/.

[79] Radio Free Europe, "China Closes 'Porn' Sites," Radio Free Europe, April 1, 2009.

[80] For example, in June 2006, the Information Office under the State Council and the MII embarked on a period of "strict supervision" of search engines, chat rooms, and blog service providers to curb the circulation of "harmful" information online. Xinhua News Agency, "China to tighten supervision over blogs, online search engines," June 29, 2006. See also Howard French, "Chinese discuss plan to tighten restrictions on cyberspace ," *The New York Times*, July 4, 2006.

[81] China Internet Network Information Center, "Twenty-third Statistical Survey Report on the Internet Development in China," issued March 23, 2009, (Chinese version).

[82] China Internet Network Information Center, "Twenty-third Statistical Survey Report on the Internet Development in China," issued March 23, 2009, http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf.

[83] David Shambaugh, CHINA'S PROPAGANDA SYSTEM: INSTITUTIONS, PROCESSES AND EFFICACY, THE CHINA JOURNAL, NO. 57, JANUARY 2007, p. 25-58.

[84] Interview with editor of a national online portal, XX 2007. *See also* Rebecca MacKinnon, "China's Censorship 2.0: How companies censor bloggers," First Monday [Online], Volume 14 Number 2 (25 January 2009), http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089.

[85] Article 2, *Provisions on the Administration of News Information Services,* issued by the Ministry of Information Industry and the State Council Information Office on September 25, 2005, http://www.isc.org.cn/20020417/ca315779.htm (Chinese), unofficial English

translation at http://www.cecc.gov/pages/virtualAcad/index.phpd?showsingle=24396.

86 Article 15, *Provisions on the Administration of News Information Services,* issued by the Ministry of Information Industry and the State Council Information Office on September 25, 2005, http://www.isc.org.cn/20020417/ca315779.htm (Chinese), unofficial English translation at http://www.cecc.gov/pages/virtualAcad/index.phpd?showsingle=24396.

87 Article 2, *Provisions on the Administration of News Information Services,* issued by the Ministry of Information Industry and the State Council Information Office on September 25, 2005, http://www.isc.org.cn/20020417/ca315779.htm (Chinese), unofficial English translation at http://www.cecc.gov/pages/virtualAcad/index.phpd?showsingle=24396.

88 Article 11, *Provisions on the Administration of News Information Services,* issued by the Ministry of Information Industry and the State Council Information Office on September 25, 2005, http://www.isc.org.cn/20020417/ca315779.htm (Chinese), unofficial English translation at http://www.cecc.gov/pages/virtualAcad/index.phpd?showsingle=24396.

89 See Benjamin Liebman, "Watchdog or demagogue? The media in the Chinese legal system," *The Columbia Law Review*, January 2005, p. 41.

90 *See* Stephanie Wang and Robert Faris, "Welcome to the Machine," Index On Censorship,. (Volume 37, Issue 2 May 2008), pages 106 – 113.

91 Anne S.Y. Cheung, THE BUSINESS OF GOVERNANCE: CHINA'S LEGISLATION ON CONTENT REGULATION IN CYBERSPACE, New York University Journal of International Law and Politics, Fall 2005-Winter 2006, 38 N.Y.U. J. Int'l L. & Pol. 1.

92 China Human Rights Defenders, Tug of War over China's Cyberspace: A Sequel to Journey to the Heart of Censorship (Part II), March 19, 2009, http://crd-net.org/Article/Class9/Class11/200903/20090319000543_14370.html.

93 Reporters Without Borders, "2009 Annual Report: China," http://www.rsf.org/en-rapport57-China.html.

94 China Human Rights Defenders, "Tug of War over China's Cyberspace: A Sequel to Journey to the Heart of Censorship (Part II)," March 19, 2009, http://crd-net.org/Article/Class9/Class11/200903/20090319000543_14370.html.

95 Chinese Human Rights Defenders, "Annual report on Chinese Internet Surveillance (2007)" (*Zhongguo Wangluo Jiankong Yu Fanjiankong Niandu Baogao*), http://www.crd-net.org/Article/Class1/200807/20080710165332_9340.html.

96 Reporters Without Borders, "Journalist gets four years for exposing Communist Party corruption in Shandong", May 2008, http://www.rsf.org/article.php3?id_article=27034.

97 Human Rights in China Press Release, "Family Visits Still Denied to Sichuan School Teacher Punished after Quake-Zone Visit," July 29, 2008, http://www.hrichina.org/public/contents/press?revision_id=66556&item_id=66524.

98 Article13, Rules on the Management of Internet Electronic Bulletin Services (*Hulianwang dianzi gonggao fuwu guanli guiding)*, issued by the Ministry of Information Industry on October 7, 2000.

99 Article 20, Measures for Managing Internet Information Services (*Hulianwang xinxi fuwu guanli banfa),* issued by the State Council on September 25, 2000, effective October 1, 2000.

100 OpenNet Initiative blog, "China incentivizes self-censorship in regulation of online video," January 4, 2008, http://opennet.net/blog/2008/01/china-incentivizes-self-censorship-regulation-online-video.

101 Article 9, *Provisions on the Management of Internet Audio and Video Programming Services*, issued by the State

Administration of Radio, Film and Television (SARFT) and the Ministry of Information Industry of the People's Republic of China on December 20, 2007, effective January 31, 2008, unofficial translation available at http://opennet.net/news/china-provisions.

102 Article 2, *Provisions on the Administration of News Information Services,* issued by the Ministry of Information Industry and the State Council Information Office on September 25, 2005, unofficial English translation at http://www.cecc.gov/pages/virtualAcad/index.phpd?showsingle=24396.

103 SARFT Notice for Strengthening the Administration of Internet Audio and Video Programming Content (*guangdian zongju guanyu jiaqiang hulianwang shiting jiemu neirong guanli de tongzhi*), issued March 30, 2009, http://www.sarft.gov.cn/articles/2009/03/30/20090330171107690049.html.

104 Section 2(1-21), SARFT Notice for Strengthening the Administration of Internet Audio and Video Programming Content (*guangdian zongju guanyu jiaqiang hulianwang shiting jiemu neirong guanli de tongzhi*), issued March 30, 2009, http://www.sarft.gov.cn/articles/2009/03/30/20090330171107690049.html. Unofficial translation at Danwei, "New rules imposed on Internet video content," April 1, 2009, http://www.danwei.org/media_regulation/new_rules_imposed_on_internet.php.

105 Section 3, SARFT Notice for Strengthening the Administration of Internet Audio and Video Programming Content (*guangdian zongju guanyu jiaqiang hulianwang shiting jiemu neirong guanli de tongzhi*), issued March 30, 2009, http://www.sarft.gov.cn/articles/2009/03/30/20090330171107690049.html. Unofficial translation at Danwei, "New rules imposed on Internet video content," April 1, 2009,
http://www.danwei.org/media_regulation/new_rules_imposed_on_internet.php.

106 Article 23, *Provisions for the Management of Internet Audio and Video Programming Services*, issued by the State Administration of Radio, Film and Television (SARFT) and the Ministry of Information Industry of the People's Republic of China on December 20, 2007, effective January 31, 2008, unofficial translation available at http://opennet.net/news/china-provisions.

107 Paul Budde Communication Pty Ltd., "China-New Internet Economy," April 24, 2009.

108 Interactive Investor, "China orders 8 more online video-sharing web sites to shut down", May 2008, http://www.iii.co.uk/news/?type=afxnews&articleid=6721662&action=article.

109 Jonathan Richards, "'Chinese YouTube' shut down amid censor fears," Times Online, June 20, 2008, http://technology.timesonline.co.uk/tol/news/tech_and_web/article4179103.ece; Loretta Chao, "Closure of Chinese Online-Video Site Sparks Concern," The Wall Street Journal, June 20, 2008, http://online.wsj.com/article/SB121390202591089267.html?mod=2_1567_leftbox. 56.com was issued an Internet video provider license in December 2008. Reuters, "Vobile Announces Commercial Deployment With Leading Video Sharing Website 56.com," March 23, 2009, http://www.reuters.com/article/pressRelease/idUS95209+23-Mar-2009+PRN20090323.

110 Steven Schwankert, "China Approves Video Site Youku's License," July 10, 2008, IDG News Service, http://pcworld.about.com/od/interne1/China-Approves-Video-Site-Youk.htm.

111 China Internet Network Information Center, "Twenty-third Statistical Survey Report on the Internet Development in China," issued March 23, 2009, http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf.

[112] *See* Stephanie Wang and Robert Faris, "Welcome to the Machine," Index On Censorship,. (Volume 37, Issue 2 May 2008), pages 106-113.

[113] Roland Soong, "The Weng'an Mass Incident," EastSouthWestNorth blog, July 1, 2008, http://www.zonaeuropa.com/20080701_1.htm.

[114] Bob Chen, "China: Let's do push-up!" Global Voices Online, July 7, 2008, http://globalvoicesonline.org/2008/07/07/china-lets-do-push-up/.

[115] Roland Soong, "The Weng'an Mass Incident," EastSouthWestNorth blog, July 1, 2008, http://www.zonaeuropa.com/20080701_1.htm.

[116] Xinhua News Agency, "Police station assaulted, torched by local people in southwest China county," June 20, 2009, http://news.xinhuanet.com/english/2008-06/29/content_8456602.htm.

[117] ONI blog, "China's Net Nannies in full force after riot in Southern China," July 2, 2008, http://opennet.net/blog/2008/07/china%E2%80%99s-net-nannies-full-force-after-riot-southern-china.

[118] Jonathan Ansfield, "Guizhou Riots: How much steam can the machine filter?," Newsweek blog, July 2, 2008, http://blog.newsweek.com/blogs/beijing/archive/2008/07/02/can-the-propaganda-machine-filter-the-steam.aspx. OpenNet Initiative Blog, "China's Net Nannies in full force after riot in Southern China," July 2, 2008, http://opennet.net/blog/2008/07/china%E2%80%99s-net-nannies-full-force-after-riot-southern-china.

[119] OpenNet Initiative Blog, "China's Net Nannies in full force after riot in Southern China," July 2, 2008, http://opennet.net/blog/2008/07/china%E2%80%99s-net-nannies-full-force-after-riot-southern-china.

[120] Roland Soong, "The Weng'an Mass Incident," EastSouthWestNorth blog, July 1, 2008, http://www.zonaeuropa.com/20080701_1.htm.

[121] "Final autopsy shows girl in southwest China protest drowned," Xinhua, July 10, 2008, http://news.xinhuanet.com/english/2008-07/10/content_8519852.htm.

[122] Rebecca MacKinnon, "China's Censorship 2.0: How companies censor bloggers," First Monday [Online], Volume 14 Number 2 (25 January 2009), http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089.

[123] Nart Villeneuve, Search Monitor Project: Toward a Measure of Transparency, June 2008, http://www.citizenlab.org/papers/searchmonitor.pdf.

[124] Nart Villeneuve, Search Monitor Project: Toward a Measure of Transparency, June 2008, p. 19, http://www.citizenlab.org/papers/searchmonitor.pdf.

[125] "Baidu's Internal Monitoring and Censorship Document Leaked (1) (Updated)," China Digital Times, http://chinadigitaltimes.net/2009/04/baidus-internal-monitoring-and-censorship-document-leaked/.

[126] See, e.g., http://chinagfw.org/2009/04/blog-post_5218.html.

[127] "Chinese Censors Cut Off Twitter, Hotmail and Flickr (Updated)," China Digital Times, http://chinadigitaltimes.net/2009/06/chinese-censors-cut-off-twitter-hotmail-and-flickr/.

[128] Isaac Mao, "Meta: Great Firewall vs. Social Media," March 6, 2009, http://www.isaacmao.com/meta/2009/03/great-firewall-vs-social-media.html.

[129] Foreign Ministry Spokesperson Liu Jianchao's Regular Press Conference, December 16, http://www.chinaconsulatechicago.org/eng/fyrth/t526582.htm.

[130] China Internet Illegal Information Reporting Centre, http://ciirc.china.cn/.

[131] Xinhua News Agency, "Seven departments launch operation for fixing the spread of

vulgarity on the Internet," (*qi bumen kaizhan zhengzhi hulianwang disu zhifeng xingdong*), January 5, 2009, http://www.gov.cn/jrzg/2009-01/05/content_1196447.htm.

[132] Article 41, CONSTITUTION OF THE PEOPLE'S REPUBLIC OF CHINA, http://english.peopledaily.com.cn/constitution/constitution.html.

[133] See, e.g. "China's Emerging Land Rights Movement," China Digital Times, December 22, 2007, http://chinadigitaltimes.net/2007/12/chinas-emerging-land-rights-movement/.

[134] Joshua Rosenzweig, "China's Battle Over the Right to Criticize," May 1, 2009, http://www.feer.com/essays/2009/may/chinas-battle-over-the-right-to-criticize.

[135] Cai Ke, "Wrongly-jailed blogger fights for justice," China Daily, May 20, 2009, http://www.chinadaily.com.cn/china/2009-05/20/content_7793902.htm.

[136] "Update: Review Underway in Wu Baoquan's Case," April 22, 2009, http://siweiluozi.blogspot.com/2009/04/update-review-underway-in-wu-baoquans.html; see all posts from Siweiluozi's Blog on Wang Shuai at http://siweiluozi.blogspot.com/search/label/Wang%20Shuai.

[137] Joshua Rosenzweig, "China's Battle Over the Right to Criticize," May 1, 2009, http://www.feer.com/essays/2009/may/chinas-battle-over-the-right-to-criticize.

[138] Joshua Rosenzweig, "China's Battle Over the Right to Criticize," May 1, 2009, http://www.feer.com/essays/2009/may/chinas-battle-over-the-right-to-criticize.

[139] Jane Chen, "Officials punished over land scandal," Shanghai Daily, April 29, 2009, http://www.shanghaidaily.com/sp/article/2009/200904/20090429/article_399326.htm.

[140] EastSouthWestNorth blog, "The First 'Human Flesh Search' Trial," August 2, 2008, http://www.zonaeuropa.com/20080802_1.htm.

[141] EastSouthWestNorth blog, "The First 'Human Flesh Search' Trial," August 2, 2008, http://www.zonaeuropa.com/20080802_1.htm.

[142] Reuters, "Man wins case vs 'human flesh search engine,'" December 19, 2008, http://www.reuters.com/article/technologyNews/idUSTRE4BI1I620081219.

[143] China Journal blog, "A Verdict in the Case of the 'Human Flesh Search Engine,'" Wall Street Journal, December 19, 2008, http://blogs.wsj.com/chinajournal/2008/12/19/a-verdict-in-the-case-of-the-human-flesh-search-engine/.

[144] Caijing.com, "Webmasters Found Guilty of Online Harassment," December 22, 2008, http://english.caijing.com.cn/2008-12-22/110041383.html.

[145] "Court decision in 'human flesh search engine' case," January 13, 2009, http://lawprofessors.typepad.com/china_law_prof_blog/2009/01/court-decision.html.

[146] Xinhua News Agency, "Law urged to protect personal information," March 4, 2009, http://www.china.org.cn/government/NPC_CPPCC_2009/2009-03/04/content_17371338.htm; Xinhua News Agency, "Law amendments adopted to protect personal information, punish bribe-taking relatives of officials," February 28, 2008, http://news.xinhuanet.com/english/2009-02/28/content_10916168.htm; Li Xinran, "Xuzhou shuts down 'human flesh search engine'" Shanghai Daily, January 20, 2009, http://www.shanghaidaily.com/sp/article/2009/200901/20090120/article_388687.htm.

[147] Forbes, "Who will be watching you in Beijing?," http://www.forbes.com/travel/2008/07/08/olympics-security-privacy-forbeslife-olympics08-cx_rr_0708security.html, July 08, 2008.

[148] Ministry of Public Security, "National Development and Reform Commission issues national approval for the 'Golden Shield' construction project at management conference," (*guojia*

fazgaiwei zhuchi zhaokai dahui tongguo "jindun gongcheng" jianshe xiangmu guojia yanshou) 国家发改委主持召开大会通过"金盾工程"建设项目国家验收), November 17, 2006, http://www.mps.gov.cn/cenweb/brjlCenweb/jsp/common/article.jsp?infoid=ABC00000000000035645. See also Greg Walton, "China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China," a Rights and Democracy Report, October 2001, http://www.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html.

149 "Safe-City Project Home For New Chinese IP Video Surveillance Technology," China Tech News, March 11, 2008, http://www.chinatechnews.com/2008/03/11/6475-safe-city-project-home-for-new-chinese-ip-video-surveillance-technology/; "China Security & Surveillance Announces Additional Safe City Project Win in Yinchuan City," Reutuers, June 30, 2008, http://www.reuters.com/article/pressRelease/idUS125704+30-Jun-2008+PRN20080630.

150 Kathrin Hille, "China bolsters internet censors' scrutiny," Financial Times, January 5 2009, http://www.ft.com/cms/s/0/f858f9aa-dac8-11dd-8c28-000077b07658,dwp_uuid=9c33700c-4c86-11da-89df-0000779e2340.html.

151 TRS Information Technology, http://www.trs.com.cn/en/TRS/about/.

152 TRS Information Technology, http://www.trs.com.cn/en/TRS/about/.

153 Article 3, *Measures for the Management of Email Services* (*huliangwang dianzi youjian fuwu guanli banfa*), issued by the Ministry of Information Industry on November 7, 2005, effective March 30, 2006.

154 Chinese cyber-dissidents and activists, such as the journalist Shi Tao, have been convicted in part because of some email service providers' disclosure of their users' personal information to the Chinese police. Reporters Without Borders, Press Release, "Cyber-dissident convicted on Yahoo! information is freed after four years," November 9, 2006, http://www.rsf.org/article.php3?id_article=8453. See also Human Rights in China Case Highlight, Shi Tao and Yahoo, at http://hrichina.org/public/highlight/index.html.

155 *See* Dui Hua News Blog, "Police Document Sheds Additional Light on Shi Tao Case," July 25, 2007, http://www.duihua.org/2007/07/police-document-sheds-additional-light.html.

156 Human Rights Watch Backgrounder, Freedom of Expression and the Internet in China, http://www.hrw.org/backgrounder/asia/china-bck-0701.htm; Alfred Hermida, "Behind China's Internet red firewall," BBC News Online, September 3, 2002, http://news.bbc.co.uk/1/low/technology/2234154.stm.

157 Washington Post, "Chinese Crack Down On Student Web Sites", March 24, 2005, http://www.washingtonpost.com/ac2/wp-dyn/A61334-2005Mar23?language=printer.

158 Xinhua News Agency, "Internet real-name registration system: Why so difficult to implement? An Investigation into the implementation of the Hangzhou Regulations for Network Security Protection," May 19, 2009, http://news.xinhuanet.com/newscenter/2009-05-19/content_11399392.htm; David Bandurski, "Xinhua: Hangzhou's "real-name Web registration system" is "on the shelf"," China Media Project, May 20, 2009, http://cmp.hku.hk/2009/05/20/1632/.

159 "Beijing Mobile's Plan for Real Name Registration for Easyown Cell Phone Numbers," China Digital Times, http://chinadigitaltimes.net/2008/01/beijing-mobiles-plan-for-real-name-registration-for-easyown-cell-phone-numbers/.

160 Article 14, Measures for Managing Internet Information Services (*Hulianwang xinxi*

fuwu guanli banfa), issued by the State Council on September 25, 2000, effective October 1, 2000.

161 China Internet Network Information Center, "Twenty-third Statistical Survey Report on the Internet Development in China," issued March 23, 2009, p. 27 (Chinese version).

162 Articles 19, 21, 23, Regulations on the Administration of Business Sites Providing Internet Services (*Hulianwang shangwang fuwu guanye changsuo guanli tiaolie),* issued by the State Council on September 29, 2002, effective November 15, 2002.

163 Article 14, Rules on the Management of Internet Electronic Bulletin Services (*Hulianwang dianzi gonggao fuwu guanli guiding),* issued by the Ministry of Information Industry on October 7, 2000, effective.

164 Chinese Human Rights Defender, "How does government monitor our online communication?" (*Zhengfu Ruhe Jiankong Women De Dianzi Wangluo Tongxu*), http://crd-net.org/Article/Class1/200803/2008032 4093843_8168.html.

165 Chinese Human Rights Defender, "How does government monitor our online communication?" (*Zhengfu Ruhe Jiankong Women De Dianzi Wangluo Tongxu*), http://crd-net.org/Article/Class1/200803/2008032 4093843_8168.html.

166 Nart Villeneuve, BREACHING TRUST: An analysis of surveillance and security practices on China's TOM-Skype platform, Information Warfare Monitor and ONI Asia Joint Report, October 1, 2008, http://www.infowar-monitor.net/breachingtrust/.

167 John Markoff, "Surveillance of Skype Messages Found in China," The New York Times, October 1, 2008, http://www.nytimes.com/2008/10/02/te chnology/internet/02skype.html?pagewan ted=all.

168 Sky Canaves, "Skype Responds to China Surveillance Report," The Wall Street Journal Blogs-China Journal, October 2, 2008, http://blogs.wsj.com/chinajournal/2008/ 10/02/skype-response-on-china-surveillance-report/?mod=googlenews_wsj.

169 Sumner Lemon, "China tightens surveillance of Internet forums," The Standard, March, 2005, http://archive.thestandard.com/internetn ews/002807.php.

170 Reporters Without Borders, "Living dangerously on the Net," May, 2003, http://www.rsf.org/article.php3?id_article =6793.

171 Washington Post, "Chinese crack down on student web sites", March 24, 2005, http://www.washingtonpost.com/ac2/wp-dyn/A61334-2005Mar23?language=printer.

172 Australia Broadcasting Corporation, "China's mobile network: a big brother surveillance tool?," January 28, 2008, http://www.abc.net.au/news/stories/200 8/01/28/2147712.htm.

173 China Business Daily, "Regulation on the Management of Short Message Service will soon come into being," (*Tongxin Duanxiaoxi Fuwu Guanli Guiding Jijiang Chutai*), March 27, 2008, http://www.txxxb.com/news/article.php?i d=7544; Australia Broadcasting Corporation, "China's mobile network: a big brother surveillance tool?," Jan 28, 2008, http://www.abc.net.au/news/stories/200 8/01/28/2147712.htm; Also see Chinese Human Rights Defenders, "How does government monitor our online communication?" (*Zhengfu Ruhe Jiankong Women De Dianzi Wangluo Tongxu*), http://crd-net.org/Article/Class1/200803/2008032 4093843_8168.html.

174 Ibid.

175 Ibid.

176 Brian Krebs, "Cyber Attacks Target Pro-Tibet Groups," Washington Post, March 21, 2008, http://www.washingtonpost.com/wp-

dyn/content/article/2008/03/21/AR2008032102605.html.

177 Information Warfare Monitor, Tracking GhostNet: Investigating a Cyber Espionage Network, March 29, 2009, http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.

178 Human Rights Watch, "China's Olympian Human Rights Challenges: In the Words of Chinese Officials," http://china.hrw.org/in_the_words_of_chinese_officials.

179 Xinhua News Agency, "Openness to foreign media to remain after Games, July 30, 2008, http://www.chinadaily.com.cn/china/2008-07/30/content_6890786.htm.

180 Jacquelin Magnay, "Fury vented at great firewall of China," The Sydney Morning Herald, July 28, 2008, http://www.smh.com.au/news/beijing2008/reporters-vent-fury-at-great-firewall-of-china/2008/07/27/1217097058479.html.

181 Katie Thomas, "Officials investigate reports of censorship at Olympic Press Center," NYTimes Blog: 2008 Beijing Olympics and Paralympics, July 29, 2008, http://olympics.blogs.nytimes.com/2008/07/29/officials-investigate-reports-of-censorship-at-olympic-press-center/?hp.

182 Nick Mulvenney, "UPDATE 1-Olympics-IOC admits to deal with China on censorship," Reuters, July 30, 2008, http://www.reuters.com/article/olympicsNews/idUSPEK15086520080730?sp=true.

183 Xinhua News Agency, "Beijing Olympic press centers open," July 8, 2008, http://news.xinhuanet.com/english/2008-07/08/content_8509880.htm.

184 Keith Bradsher, "China Blocks Access to The Times's Web Site," The New York Times, December 19, 2008, http://www.nytimes.com/2008/12/20/world/asia/20china.html.

185 Miguel Helft, "YouTube Blocked in China," New York Times, March 24, 2009, http://www.nytimes.com/2009/03/25/technology/internet/25youtube.html?_r=1&hp.

186 Herdict, "www.blogger.com in China," http://www.herdict.org/web/explore/detail/id/CN/2488.

187 Tania Branigan, "China blocks Twitter, Flickr and Hotmail ahead of Tiananmen anniversary," The Guardian (UK), June 2, 2009, http://www.guardian.co.uk/technology/2009/jun/02/twitter-china.

188 See Rebecca MacKinnon, "Original government document ordering "Green Dam" software installation," June 8, 2009, http://rconversation.blogs.com/rconversation/2009/06/original-government-document-ordering-green-dam-software-installation.html.

189 "Notice Regarding the Pre-Installation of "Green" Online Filtering Software on Computers (关于计算机预装绿色上网过滤染件的通知,*guanyu jisuanji yuzhuang luse shangwang guolu ranjian de tongzhi*)," Ministry of Industry and Information Technology Notice No. 226 [2009], May 19, 2009, http://tech.sina.com.cn/it/2009-06-09/17073163327.shtml., unofficial translation at http://www.hrichina.org/public/contents/press?revision_id=169834&item_id=169820; Xinhua News Agency, "Anti-porn filter software stirs up disputes in China," June 11, 2009, http://news.xinhuanet.com/english/2009-06/11/content_11522822.htm.

190 "Notice Regarding the Pre-Installation of "Green" Online Filtering Software on Computers (关于计算机预装绿色上网过滤染件的通知,*guanyu jisuanji yuzhuang luse shangwang guolu ranjian de tongzhi*)," Ministry of Industry and Information Technology Notice No. 226 [2009], May 19, 2009, http://tech.sina.com.cn/it/2009-06-09/17073163327.shtml.

191 OpenNet Initiative Bulletin, "China's Green Dam: The Implications of Government Control Encroaching on the Home PC," June 12, 2009,

http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc.

[192] *Ibid.*

[193] *Ibid.* See also Hal Roberts, "China Bans the Letter 'F,'" June 12, 2009, http://blogs.law.harvard.edu/hroberts/2009/06/12/china-bans-the-letter-f/.

[194] *Ibid*.

[195] Scott Wolchok, Randy Yao, and J. Alex Halderman, "Analysis of the Green Dam Censorware System," Computer Science and Engineering Division, The University of Michigan, Revision 2.4, June 11, 2009, http://www.cse.umich.edu/~jhalderm/pub/gd/.

[196] OpenNet Initiative Bulletin, "China's Green Dam: The Implications of Government Control Encroaching on the Home PC," June 12, 2009, http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc.