Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**305**
Land:	Kina
Kilde:	Freedom House
Titel:	Freedom on the Net 2012 – China
Udgivet:	25. september 2012
Optaget på baggrundsmaterialet:	20. december 2012

Title	Freedom on the Net 2012 - China
Publisher	Freedom House
Country	China
Publication Date	25 September 2012
Cite as	Freedom House, *Freedom on the Net 2012 - China*, 25 September 2012, available at: http://www.unhcr.org/refworld/docid/5062e8a8c.html [accessed 11 December 2012]
Disclaimer	This is not a UNHCR publication. UNHCR is not responsible for, nor does it necessarily endorse, its content. Any views expressed are solely those of the author or publisher and do not necessarily reflect those of UNHCR, the United Nations or its Member States.

Freedom on the Net 2012 - China

INTERNET FREEDOM STATUS	2011 Not Free	2012 Not Free
Obstacles to Access (0-25)	19	18
Limits on Content (0-35)	28	29
Violations of User Rights (0-40)	36	38
Total (0-100)*	83	85

* 0=most free, 100=least free

POPULATION: 1.3 billion
INTERNET PENETRATION 2011: 38 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
NOTABLE POLITICAL CENSORSHIP: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

Introduction

Although China is home to the world's largest population of internet users, many of whom have shown increasing creativity in pushing back against censorship, the country's internet environment remains one of the world's most restrictive. This reflects the Chinese Communist Party's paradoxical "two-hand strategy" for managing digital technologies: promoting access for the purposes of economic advancement on the one hand while attempting to secure control over content, especially political communication, on the other.[1]

This paradox was especially evident in 2011 and early 2012. On the one hand, the Chinese authorities further enhanced an already sophisticated and multilayered system for censoring, monitoring, and manipulating activities on the internet, while abducting or imprisoning dozens of activists, lawyers, and bloggers. The scale and speed of the censorship effort – particularly the use of tens of thousands of human censors to identify and delete social media posts – was remarkable. One academic study reviewing censorship across nearly 1,400 blog-hosting and bulletin-board platforms in China estimated that 13 percent of posts were deleted, many within 24 hours of a particular term becoming sensitive or indicating collective action potential.[2] Such controls contributed to the Chinese internet increasingly resembling an intranet. Many average users, isolated from international social media platforms and primarily exposed to a manipulated online information landscape, have limited knowledge of key events making news around the globe, including the publication of diplomatic cables by the antisecrecy group Wikileaks or anti-government protest movements sweeping the Middle East. Meanwhile, as one of the biggest domestic political scandals in recent memory unfolded in early 2012, many Chinese users were similarly left in the dark about events affecting the upcoming Communist Party's once-in-a-decade leadership change.

At the same time, due to the egalitarian nature and technical flexibility of the internet, the online environment remains freer and Chinese citizens more empowered than what is possible in the traditional media sector. Although Twitter remains blocked in China, a growing number of Chinese users are circumventing censorship to reach it and other restricted sites. Meanwhile domestic microblogging services like Sina Weibo have grown rapidly, surpassing 300 million users by early 2012. Their influence as a source of news and an outlet for public opinion has correspondingly grown. Microblogs' speed of transmission and other censorship loopholes enabled netizens to outpace censors, draw attention to incipient scandals, and mount online campaigns on various topics. The authorities responded with tightened controls on such services, including intensified censorship and real-name registration requirements, although the new restrictions' full effect on online discourse remains to be seen.

The Chinese public was first granted access to the internet in 1996, and the number of users has grown exponentially, from 20 million in 2001 to over 500 million in 2011.[3] Since it was first introduced, however, the ruling Chinese Communist Party (CCP) has consistently sought to assert its authority over the new medium. The underlying system of infrastructural control and filtering technology has been more or less complete since 2003,[4] while more sophisticated forms of censorship and manipulation have gained prominence recently.

Obstacles to Access

While the role and presence of information and communication technologies (ICTs) has continued to grow, users still face key obstacles to full and free access. These include centralized control over international gateways, a notable urban-rural gap, and sporadic, localized shutdowns of internet access at sites of protest.

The rate of internet adoption in China has slowed in recent years, as the market in urban areas begins reach a saturation point and most of the people with the literacy, interest, and economic capacity to use the internet are already online.[5] The government-linked China Internet Network Information Center (CNNIC) estimated in March 2012 that there were a total of 527 million users in the country, an increase of over 70 million since the end of 2010.[6] Given the country's large population and uneven economic development, however, the overall penetration rate remains just 39.4 percent,[7] slightly higher than the global average in 2011 (around 35 percent).[8] The average penetration rate in urban areas (73.5 percent) is over 45 points higher than that in rural areas (26.5 percent); in 2007, the gap was approximately 20 percentage points, suggesting a widening divide.[9]

Most users access the internet from home or work, with fewer using cybercafes than in the past, though these still account for 26.7 percent of users.[10] The vast majority of internet connections are via broadband rather than dial-up,[11] although access to international websites is slow due to the burden caused by the nationwide filtering and monitoring system.[12] Though generally affordable in urban areas, broadband prices are expected to drop in the near future. In the aftermath of an investigation into their dominance over the broadband market, telecommunications giants China Telecom and China Unicom announced in December 2011 that over the next five years, they would substantially raise broadband speeds while at the same time lowering costs.[13]

Use of mobile telephones has spread faster than internet access. According to the International Telecommunication Union (ITU), there were about 986 million mobile phone users in China at the end of 2011 – an increase of 100 million over 12 months – giving the country a penetration rate of about 73 percent and the world's largest population of mobile users.[14] Access to the internet via mobile phones is rapidly gaining popularity. By November 2011, 318 million people used this service,[15] often for accessing domestic microblogging applications offered by Sina, Tencent, Sohu, and other companies; CNNIC estimated that over 45 percent of Chinese internet users had signed up for one of these microblogging services by the end of 2011.[16]

The Chinese government has been known to shut down access to entire communications systems in response to specific events. The most dramatic such incident occurred in Xinjiang after an outburst of ethnic violence in the region's capital Urumqi; the blackout lasted from July 2009 to May 2010.[17] Since then, the authorities have similarly shut down internet communications at sites of unrest though on a smaller scale and lasting for shorter periods of time (usually several days or weeks): in December 2011, around the village of Wukan in Guangdong, after residents revolted against local officials over illegal land grabs;[18] and in February 2012 in Tibetan areas of Sichuan, after clashes surrounding a series self-immolations and reports that soldiers had opened fire on civilians.[19] In a partial shut down, beginning May 30, 2011, nearly all Mongolian chat rooms, discussion forums, blogs and instant messaging platforms, as well as many text-messaging services, were shut down for about a month in Inner Mongolia surrounding protests that erupted after a Mongolian herder was killed.[20]

Internet access service, once monopolized by China Telecom, has been liberalized and decentralized, and users can now choose from among scores of private internet service providers (ISPs). The government has been willing to liberalize the ISP market in part because of the centralization of the country's connection to the international internet, which is controlled by six to eight state-run operators that maintain advanced international gateways in Beijing, Shanghai, and Guangzhou.[21] This arrangement remains the primary infrastructural limitation on open internet access in the country, as all ISPs must subscribe via the gateway operators and obtain a license from the Ministry of Industry and Information Technology (MIIT). The system essentially creates a national intranet and gives the authorities the ability to cut off any cross-border information requests that are deemed undesirable. Mobile telephone communication is dominated by three state-owned operators: China Mobile, China Telecom, and China Unicom. Under the oversight of the MIIT, connection to the internet via mobile phones is also monitored by the international gateway operators.

The authorities have sought to exercise increasingly tight control over the cybercafe business and other public access points. The issuance of cybercafe licenses is managed by the Ministry of Culture and its local departments, although to obtain a license, a proprietor typically must also communicate with various other state entities.[22] In January 2011, the Vice Minister of Culture announced that all sole-proprietor cybercafes would be replaced by chains within the next five years, a move that observers believed was aimed at increasing the efficiency of surveillance and censorship.[23] By December 2011, 40 percent of cybercafes in China were reportedly be owned

by chains.[24] In another development affecting internet access in public spaces, in July 2011, police in central Beijing's Dongcheng district announced that all cafes, hotels, and other businesses offering wireless internet access must install surveillance software or face penalties and possible closure.[25] Some small business owners cut off their wireless service to avoid paying for the mandatory software (which cost about US$3,000), though some others reportedly ignored the directive.[26]

Limits on Content

The Chinese authorities continue to employ the most elaborate system for internet content control in the world. Government agencies and private companies together employ hundreds of thousands of people to monitor, censor, and manipulate online content. In recent years, additional layers have been added to this apparatus, particularly as the CCP seeks to restrict the use of social-networking and microblogging applications for political mobilization and sharing of uncensored information. Even this heavily censored and manipulated online environment, however, provides more space for average citizens to express themselves and air their grievances against the state than any other medium in China.

The CCP's content-control strategy consists of three primary techniques: automated technical filtering, forced self-censorship by service providers, and proactive manipulation. These techniques mutually reinforce each other to create a highly manipulated information landscape and one notably isolated from international news flows. The purported goal is to limit the spread of pornography, gambling, rumors, and other harmful practices, but web content related to sensitive political or social topics is targeted at least as forcefully.[27] The most systematically censored topics include criticism of top leaders, independent evaluations of China's rights record, violations of minority rights in Tibet[28] and Xinjiang, the Falun Gong spiritual group, the 1989 Beijing massacre, and various dissident initiatives that challenge the regime on a systemic level.[29] These standing taboos are supplemented by almost daily directives on negative developments, budding civic movements, or other forms of collective action. Criticism of the censorship system is also heavily censored.[30] In 2011, directives restricted reporting on a fatal high-speed rail collision, antigovernment protests in the Middle East, nuclear leaks related to the earthquake in Japan, tainted food scandals, environmental disasters, ethnic protests in Inner Mongolia,[31] and efforts by hundreds of independent candidates to run for seats on local people's congresses. Users' venting frustration at local governments or broader politically oriented terms like "democracy," "human rights," and "freedom of speech" are subject to less extensive censorship,[32] and according to one study, their prevalence in the Chinese blogosphere has grown in recent years.[33]

The first layer of the censorship apparatus is the blocking of access to foreign websites via technical filtering or what is commonly referred to as the "Great Firewall." In some cases, whole websites are blocked based on their domain name. More common, however, is the authorities' use of deep-packet inspection technologies to enable filtering of particular pages within otherwise approved sites if the pages are found to contain blacklisted keywords in the URL path.[34] This nuance renders the effect of the censorship more subtle and less noticeable to users. Filtering by keyword is also implemented in mobile phone text-messaging,[35] as well as in instant-messaging services, such as Tom-Skype and QQ, and the necessary software is built into the application upon installation.[36] Academic research indicates that since 2008 the government has upgraded the sophistication of its nationwide technical filtering equipment.[37]

In practice, one of the most important uses the government has made of technical filtering has been to impose blanket blocks on certain Web 2.0 applications, thereby isolating the Chinese public from an international network of user-generated content. Since 2009, the video-sharing platform YouTube, the social-networking site Facebook, and Twitter have remained blocked most of the time in China.[38] Other international applications have sporadically complained of disruptions, particularly at politically sensitive times. The social-networking website LinkedIn was briefly blocked in February 2011, after a discussion group related to calls for a "Jasmine Revolution" in China was created. [39] In In March, Google complained of disruptions to its Gmail email service.[40] At times, "web throttling," which slows the loading of web pages to render services nearly useless, is employed instead of a full block. Reports emerged during 2011 of web throttling being used against Google+ (a social-networking tool) [41] and the website of the anti-secrecy group Wikileaks after it published hundreds of U.S. diplomatic cables, some of which contained content normally censored in China.[42]

Simultaneously, the Chinese government has cultivated a wide range of domestic equivalents that have attracted hundreds of millions of users.[43] Chinese users thus have widespread access to video-sharing websites, social-networking tools, and email services. However, like other websites registered in China, the private Chinese companies that provide these services are required by law to ensure – either automatically or manually – that content banned by party and government censorship orders is not posted or circulated widely. Automated keyword filters are in place, but given the ease with which users can circumvent such filters via the complexities of the Chinese language, a huge percentage of deletions are implemented by human censors.[44] Editors and censorship staff reportedly receive as many as three notices per day – by text message, instant message, phone call, or email – that contain updates, adjustments, and minutiae pertaining to official censorship directives.[45] Firms risk losing their business licenses if they fail to comply, and many companies employ large staffs to carry out this task. Most postings on blogs, microblogs, comment sections of news items, and bulletin-board system (BBS) discussions that are deemed objectionable are deleted by company staff before they appear to the public or shortly thereafter. In addition, a growing army of

volunteers, tens of thousands in Beijing alone, have been recruited to assist in identifying and reporting potentially undesirable content. [46]

Two companies' required compliance with government censorship orders is especially notable because of their market dominance and the consequent impact of their actions on the online information landscape as a whole – Sina, which operates Sina Weibo, the most popular microblogging service, and Baidu, which operates the most used search engine. As of February 2012, Sina Weibo reportedly had 300 million users (of which 27 million were active daily), an exponential increase since its launch in 2009.[47] According to Sina executives, the firm has a "very powerful content censorship" system in place, which includes both automated and human monitoring 24 hours a day, run by hundreds of employees.[48] Sina Weibo users consistently report diverse measures employed by the company to prevent the circulation of politically sensitive content on a range of topics – deleting individual posts, deceiving users by making posts appear to them to have been published but actually rendering them invisible to followers, shuttering accounts, and removing results from the application's search function. For example, in September, citing government pressure, Sina shut down the account of a netizen who had used it to publish photos of Chinese ministerial-level officials wearing designer watches, a possible indication of corruption.[49] Tests conducted by Freedom House in July 2011 on the names of eight prominent human rights activists, lawyers, and journalists found that for seven of them, no results were returned to queries on Sina Weibo's search function.[50] A team of researchers from China Digital Times reportedly identified over 800 other filtered terms, including "Cultural Revolution" and "propaganda department."[51]

Baidu, which accounts for nearly 80 percent of China's search engine market,[52] has long been known to manipulate the results it offers based on government instructions, not only removing certain content, but also favoring state-approved information over content from non-governmental sources or content providers based outside of China. As an indication of the scale of information being removed, searches for the names of Gao Zhisheng, a prominent human rights lawyer who has been detained since 2010, yielded 2.25 million results on the uncensored Google.hk and only 495 on Baidu. For Ai Weiwei, an internationally renowned artist and digital activist, abducted by security forces from April to June 2011, Google.hk yielded 9.14 million results on and Baidu only 2.55 million.[53]

Foreign corporations have also been required to implement censorship of political content in order to gain access to the Chinese market. In its tests, Freedom House found that Yahoo.cn produced search results that were as heavily restricted and dominated by Chinese government links as those of Baidu, and sometimes even more restrictive. In other cases, censorship has been indirectly incorporated into foreign internet products marketed in China. After being blocked in May 2011 for aggregating content from Facebook and Twitter, Flipboard, an application for Apple's iPad tablet computer, launched a Chinese version in December 2011. The new version aggregates content from Sina Weibo, social-networking site Renren, and other Chinese brands that have already implemented censorship per government requirements.[54] In March 2010, Google announced that it would stop censoring its search results and began redirecting mainland users to its uncensored Hong Kong-based search engine after Chinese officials made it clear that "self-censorship is a nonnegotiable legal requirement."[55] The authorities responded by blocking results of searches with flagged keywords that were initiated by mainland users on the Hong Kong engine. In September 2011, the Chinese government renewed Google's license to operate in China, though its business activities have mostly focused on non-political areas like its Android smartphone platform or Adsense advertising application. [56]

Routine censorship is often temporarily reinforced surrounding politically sensitive events. Throughout 2011, news and discussion of the anti-government protests in the Middle East that ousted authoritarian leaders were sharply curtailed. Fearing similar unrest at home, Chinese leaders put the online censorship apparatus into full gear to restrict Chinese users' knowledge of the events. Words like "Egypt"[57] and "Cairo"[58] were censored on popular online portals and Weibo sites. The word "jasmine," initially used to refer to the uprising in Tunisia, became a particularly sensitive word after calls for a "Jasmine Revolution" in China appeared online. The authorities responded with wide-ranging censorship of the word, including in contexts unrelated to politics, such as references to the flower, tea, or a popular folk song. [59] In other cases, when particular posts, blog entries, or multimedia clips that authorities find offensive attract massive public attention, they may be deleted after the fact.[60]

In early 2012, some of the most notable intra-CCP infighting in decades unfolded, and its repercussions were felt in the online sphere. The political scandal was sparked in February 2012 when Chongqing's police chief Wang Lijun attempted to defect to the U.S. consulate in Chengdu. The incident ultimately resulted in the downfall of the city's party secretary Bo Xilai (a CCP heavyweight who had been eying a seat on the powerful Politburo Standing Committee), his wife's arrest for murder, rumors of a coup plot, and reports that the party's security chief Zhou Yongkang's position may be in danger. As the events unfolded, the names of these top officials joined those of rights activists, returning no search results on Sina Weibo. Leftist websites that had been supportive of Bo and his neo-Maoist propaganda were shut down.[61] In an unprecedented step in late March, Sina Weibo and Tencent's microblogging service both disabled their comment feature for three days, reportedly to allow for the "concentrated cleansing" of "rumors and other illegal and harmful information."[62] Meanwhile, reports emerged of strange behavior on Baidu, which began returning unusually open results for sensitive queries like "June 4" (a reference to the 1989 Beijing massacre) and "Wang Lijun live harvest" (a reference to allegations that Wang had been involved in the forcible harvesting of organs from Falun Gong prisoners of conscience). The openings were fleeting, but caused observers to

speculate that the CCP faction of President Hu Jintao and Premier Wen Jiabao was using Baidu to embarrass those aligned with former President Jiang Zemin by reducing censorship on human rights abuses the latter are closely associated with.[63]

Such dynamics illustrate the extent to which censorship decisions are frequently arbitrary and opaque. Some private companies are known to alert readers that content has been removed for unspecified reasons. However, attempts to access blocked URLs generally result in an error message similar to what one would encounter were a technical glitch at fault; there is no indication that content has been restricted due to a government decision. No avenue exists for appealing censorship decisions. Aware of the comprehensive nature of surveillance and censorship on the internet and mobile phone text messaging, ordinary users and bloggers engage in extensive self-censorship and often refrain from transmitting explicitly sensitive comments.

The existing censorship techniques have proven insufficient to completely overcome the flexibility of the technology, the sheer volume of communications, the creativity of users, and a sometimes intentional disregard for official directives by nonstate actors. The CCP and government agencies have taken various actions in the past year and a half to plug these gaps in the censorship system. They have included the following:

- **Creating a new agency to better coordinate internet regulation:** Over ten different government and Communist Party entities, at both the national and local level, are involved in internet censorship, with some instructions coming from the country's top leadership.[64] Much of this apparatus has remained unchanged, but in May 2011, the government also created a new agency, the State Internet Information Office (SIIO) to streamline procedures.[65] The agency was tasked with responsibilities such as managing online propaganda directives, punishing violators of online content rules, and overseeing the country's telecommunications companies.[66]

- **Increasing pressure on leading internet firms to tighten "self-discipline":** Beginning in February 2011, top officials – including several members of the powerful Communist Party Politburo Standing Committee – issued public statements or made personal visits to leading internet companies calling for tighter controls.[67] In August, the *People's Daily*, a CCP mouthpiece, published a full-page article on the political importance of controlling social media.[68] In November 2011, the SIIO organized a summit to "protect positive news online" and "reinforce self-discipline." Attending the meeting were executives of top telecommunications companies and popular websites, including China Telecom, China Mobile, China Unicom, Sina, Sohu, Netease, Baidu, and Tencent. [69] The companies were urged to stop spreading "harmful information" online and to more efficiently self-censor.

- **Tightening controls on social media, especially microblogs:** After domestic social media tools, particularly popular microblogging sites like Sina Weibo, were used to channel public anger over a fatal train crash in July and then to circulate images of thousands of urban residents in the northeast city of Dalian protesting a polluting factory in August, the government redoubled its efforts to curb their influence and ability to quickly circulate undesirable information. Under such pressure and in an attempt to encourage users to self-censor, Sina Weibo notified its subscribers in August that several microbloggers deemed to have spread unfounded rumors were having their accounts suspended for one month.[70] In other instances, Sina staff have sent "friendly" reminders to users urging them to watch their words around politically sensitive periods or have deleted posts. Users boasting a large following have come under particular scrutiny.[71] Some activists also had their accounts shutdown, mostly notably, Ai Weiwei's Sina Weibo account was blocked in August after he used it to fundraise from supporters to pay a questionable tax charge levied against him by the authorities.[72] This trend continued in early 2012, with CCP representatives placed in microblog firms,[73] a real-name registration policy initiated (see "Violations of User Rights"), and a new "user contract" that would institute a point system to keep users in line announced.[74]

Realizing that they are unable to entirely control online content and increasingly viewing cyberspace as a field for "ideological struggle,"[75] the Chinese authorities in recent years have also introduced measures to proactively sway public opinion online and amplify the party's version of events over alternative accounts. This effort has taken a number of forms.

First, online news portals are prohibited from producing their own content and are only authorized to repost information from state-run traditional media.[76] Second, in addition to removal orders, propaganda directives are often accompanied by specific instructions to marginalize or amplify certain content, particularly from state media like the official Xinhua News Agency or the *People's Daily* Communist Party mouthpiece.[77]

Third, since 2005, paid web commentators known collectively as the 50 Cent Party have been recruited to post pro-government remarks, lead online discussions in accordance with the party line, and report users who have posted offending statements. Recent accounts of their activities highlight that posts do not only praise or support the CCP and government policy, but also target government critics with negative remarks or involve deliberate attempts to muddy the facts of a particular incident, such as a sighting of police abuse.[78] Estimates from 2008 placed the number of these commentators at over 250,000, but with internet usage having doubled since then, their number has likely expanded as well.[79] Since 2009, this strategy appeared to have become both more institutionalized and more decentralized, with commentators trained and used by "government units at all levels."[80] Increasingly, government employees have been

directed to engage in online discussions to respond to criticism, though in some cases they are transparent about their ties to the state, a difference from the 50 Cent Party model. Training workshops for internet commentators were held throughout the country in 2011, including for police and prison personnel.[81]

Fourth, mobile phone communication is now treated as another medium for spreading party ideology. In 2010, a campaign was launched to encourage the dissemination of pro-government "Red text messages" through economic incentives.[82]

Despite these government restrictions, the internet has emerged in recent years as a primary source of news and forum for discussion for many Chinese, particularly among the younger generations. Chinese cyberspace is replete with online auctions, social networks, homemade music videos, a large virtual gaming population, and spirited discussion of some social and political issues.[83] Civil society organizations involved in charity, education, health care, and other social and cultural issues that are deemed acceptable by the authorities often have a dynamic online presence. The growing popularity of microblogs in 2011 amplified these dynamics and generated a strong sense of empowerment among many Chinese users at being able to directly express their opinions to large numbers of fellow citizens, even if some such posts were subsequently deleted. [84] The government's censorship of social media, which many netizens have directly encountered, has generated resentment as well. It has become increasingly common for users – including those who would not normally consider themselves politically active – to criticize censorship itself by using humor.[85]According to Xiao Qiang of China Digital Times, "the Internet has became a quasi-public space where the CCP's dominance is being constantly exposed, ridiculed, and criticized, often in the form of political satire, jokes, videos, songs, popular poetry, jingles, fiction, Sci-Fi, code words, mockery, and euphemisms."[86]

In several cases in 2011, Chinese users successfully mobilized opposition to government decisions online, prompting a change in policy. In June, officials in Nanjing revised plans for a subway expansion after an online outcry – including posts by a Sina Weibo user with five million followers – emerged claiming the plan would sacrifice too many of the city's revered Wutong trees.[87] In July, a deadly high-speed train collision in Wenzhou was first reported by Weibo users who circulated real-time reports, calls for help, and photos. When initial signs emerged that the government might be covering up the true cause of the accident and as traditional media censored coverage per official directives, public outrage erupted online – including over 25 million messages on Sina Weibo – ultimately spurring the authorities to conduct a serious investigation into the accident. [88] In other cases, incidents of corruption were exposed, strikes were organized, and kidnapped children were identified. One group of users began using Google Maps to aggregate and track incidents of forced evictions and related protests.[89] Though the authorities have yielded to public pressure in some such instances, the resulting solutions and procedures typically fall short of systemic reforms or democratic decision making and are at times complemented by increased censorship. [90]

As controls have tightened in recent years, a growing number of individuals are reportedly seeking out knowledge and techniques for circumventing censorship. According to anecdotal accounts and data obtained from managers of circumvention tools, there were spikes in usage of these tools at politically important moments in early 2012 – such as surrounding Bo Xilai's ouster or Chinese activist Chen Guangcheng's daring escape from house arrest to the U.S. embassy – when state-run media were conspicuously silent and heavy online censorship was in place. As importantly, there was an overall increase in the baseline number of users by mid-2012 when compared to late 2011, indicating that a contingent of first-time users decided to continue circumventing even during non-crisis periods.[91] In some cases, users' specific aim is to join Twitter, which is blocked in China. An activist community of some 200,000 people – an increase from 50,000 in 2010 – use the tool to rapidly transmit news, connect with other socially conscious individuals, and take advantage of an uncensored medium.[92] Such growth in the use of circumvention tools occurred despite reports throughout 2011 that the government was increasing its efforts to block users access to them.[93] Other methods for getting around censorship include using witty alternatives and homonyms for banned keywords, opening multiple blogs on different hosting sites, and using peer-to-peer technologies to circulate banned information.

Overtly political organizations, ethnic minorities, and persecuted religious groups remain underrepresented among websites that are freely accessible within China, though they have been able to use some ICTs to advance their causes. After being driven underground by a violent persecutory campaign, adherents of the Falun Gong spiritual practice have used the internet and mobile phones to maintain contact with one another and communicate with overseas practitioners. They have also downloaded censored information and disseminated it via vast amounts of offline leaflets and video discs (VCDs) that expose rights violations and cast doubt on party propaganda.[94] Tibetans have similarly used the internet and VCDs to circulate banned magazines, songs, and documentary films. Meanwhile, overseas Chinese-language media and human rights groups have reportedly sent millions of emails into the country, supplying users with news summaries on Chinese and international events, instructions on anticensorship technology, and copies of banned publications.

Violations of User Rights

Article 35 of the Chinese constitution guarantees freedoms of speech, assembly, association, and publication, but such rights are subordinated to the CCP's status as the ruling power. In addition, the constitution cannot, in most cases, be invoked in courts as a legal basis for

asserting rights. The judiciary is not independent and closely follows party directives, particularly in politically sensitive freedom of expression cases. A wide variety of regulations have been issued by different government agencies to establish censorship guidelines. The National People's Congress in April 2010 adopted an amendment to the State Secrets Law[95] that requires telecom operators and ISPs to cooperate with authorities on investigations involving the leaking of state secrets.[96] The law took effect on October 1 and has been generally met with compliance from companies, mostly because the economic stakes of disobedience and loss of business license are so high.

Vague provisions in the criminal code and state-secrets legislation have been used to imprison citizens for their online activities, including publication of articles criticizing the government or exposing human rights abuses, transmission of objectionable email messages, and downloading of censored material from overseas websites. Trials and hearings lack due process, often amounting to little more than sentencing announcements.

Prison sentences for online violations tend to be longer in China than in many other countries, often a minimum of three years and sometimes as long as life imprisonment, while punishments elsewhere typically range from six months to four years. Some users are also sentenced without trial to "reeducation through labor" camps for up to three years. Once in custody, detainees frequently suffer abuse, including torture and denial of medical attention. Though the targeted individuals represent a tiny percentage of the overall user population, the harsh sentencing of prominent figures has a chilling effect on the fairly close-knit activist and blogging community and encourages self-censorship in the broader public.

The year 2011 was notable, in particular, for a spate of extralegal abductions and long prison terms imposed in connection with online calls for a Jasmine revolution in China. The calls, which were first posted on the U.S.-based website Boxun and then spread over Twitter, sparked no serious protests, in part because of the strong show of security forces sent to the allotted sites.[97] Some observers noted, therefore, that the authorities may have used the calls as a pretext for a crackdown that had been brewing for some time as CCP officials grew wary of the growing influence of certain activists and their outspokenness online. Beginning in February 2011, dozens of lawyers, activists, and bloggers who had been active both on domestic and international social media were abducted one after another in what became one of the worst crackdowns on free expression in China in recent memory.[98] According to Chinese Human Rights Defenders, at least 78 people were known to have been taken into custody as of June 2011, either formally or extralegally.[99] In most cases, families were not notified of the detainee's whereabouts or grounds for detention. Many of the activists later reported abuse in custody, including beatings, forcible medication, sleep deprivation, and other forms of mistreatment that caused one lawyer to contract tuberculosis in only 21 days.[100]

The highest profile victim of disappearance was Ai Weiwei,[101] the prominent artist and outspoken blogger, who was abducted from early April to late June 2011. He was kept in isolation and suffered psychological pressure and threats, but no physical abuse. After his release, the authorities launched a formal prosecution on tax evasion charges, which were widely perceived as trumped up.[102] Ai and others reported being forced to sign statements promising not to be active on Twitter as a condition for their release.[103] This generated an eerie online silence for several months, but by year's end many were defying the authorities and had resumed posting to social media.[104]

Several of the individuals arrested in the crackdown were formally charged with "inciting subversion of state power" and in some cases, sentenced to long prison terms throughout the year. Ran Yunfei, a prominent blogger from Sichuan known for his advocacy of democratic reforms was charged in March 2011, but released in August and placed under house arrest on condition that he would not speak publicly. [105] Also in March, Liang Haiyi, a 35-year-old woman from Harbin, was charged with subversion after putting information about the protests in a chat room; she remained in incommunicado detention at year's end.[106] Hua Chunhui from Jiangsu was detained for "inciting subversion" after transmitting details of the revolution calls via his Twitter account and in April was sent to a "reeducation through labor camp."[107] In September, Wang Lihong, a prominent female online activist, was sentenced to nine months in prison.[108] In the most severe set of punishments, in December 2011, Chen Wei from Sichuan and Chen Xi from Guizhou were sentenced to nine and ten years in prison, respectively.[109]

More common than long-term imprisonment or abduction are other forms of extralegal harassment, including house arrest. According to some estimates, thousands of individuals have been summoned for questioning and warned in recent years by security officials, a tactic also applied in 2011 regarding the Jasmine Revolution and other issues.[110] In addition, according to Chinese Human Rights Defenders, over 80 people were placed under house arrest.[111] Even after release from prison, prominent activists have been kept under tight surveillance, house arrest, and had their internet and mobile phone connections cut of. In 2011, internationally renowned activists Hu Jia from Beijing and Chen Guangcheng from Shandong and their families were subjected to such treatment.[112] Liu Xia, the wife of democracy advocate and Nobel Peace Prize laureate Liu Xiaobo, was similarly kept under house arrest and in isolation from the outside world.[113] Liu himself remained imprisoned, serving an 11-year sentence on charges of "inciting subversion of state power" for publishing pro-democracy writings online, including drafting and circulating the prodemocracy manifesto Charter 08.[114]

The above forms of suppression were also applied during the year on topics unrelated to the Jasmine Revolution. Throughout 2011, hundreds of intellectuals, business executives, and activists attempted to compete as independent candidates in elections for local People's

Congresses, whose seats are typically secured only by candidates handpicked by the CCP. [115] Many used their Sina Weibo microblog accounts to campaign and connect with potential voters. The authorities responded with deletions, account shut downs, harassment, and occasional arrests. In May, Liu Ping from Jiangxi was detained by police,[116] while He Peng from Jiangsu was also called in for questioning. [117] Shanghai businessman Xia Shang received a visit from the Ministry of State Security and two companies he runs were "randomly" selected for a tax audit. [118] Separately, in April 2011, Fang Hung, a retired civil servant in Chongqing, was ordered to serve one year in a "re-education through labor" camp after mocking the municipal party secretary, Bo Xilai, in a microblog post.[119] Towards year's end, officials were increasingly warning users of Sina Weibo that they could face prosecution for "spreading rumors." In December 2011, state-run media reported that two men had been detained in Hunan and would be held for five days.[120] In March 2012, human rights groups reported that several people had been detained over microblog posts they published related to CCP infighting, particularly rumors of a coup attempt.[121] In recent years, local officials have also resorted to criminal defamation charges to detain and in some cases imprison whistleblowers who post corruption allegations online, though no high-profile cases were reported in 2011.

Members of religious and ethnic minorities are targeted for particularly harsh treatment for their online activities. In the aftermath of ethnic violence in Xinjiang in July 2009, several individuals involved in websites reporting on Uighur issues were sentenced to prison terms ranging from 15 years to life imprisonment. Tibetans and Falun Gong practitioners who transmit information abroad often suffer repercussions, while some have been arrested solely for accessing or quietly disseminating banned information. In January 2012, Tibetan groups reported that Gyitsang Takmig had been sentenced to four years in prison for distributing 2,500 VCDs discussing Tibetan history and aspirations for greater freedoms.[122] Some have also been detained for circulating text-messages. In Inner Mongolia, people who disseminated text-messages about widespread protests that occurred in May 2011 were summoned by the authorities.[123] According to the Falun Dafa Information Center, two women were sentenced to 5.5 and 6 years in prison in March 2011 for having sent text messages urging people to gather outside a courthouse to show solidarity during the trial of a fellow Falun Gong practitioner.[124]

The space for anonymous online communication in China is steadily shrinking as real-name registration requirements expand. Most major news portals such as Sina, Netease, and Sohu implemented real-name registration for their comment sections during 2009.[125] It had already been required in cybercafes, university BBS, and major blog-hosting sites.[126] An internet content provider (ICP) license from the MIIT is required to establish a personal or corporate website within China, and the process requires applicants to submit personal identification information. In February 2010, the authorities added a requirement that individuals registering a website have their photograph taken and placed on file.[127] In late 2011, real-name registration was expanded to domestic microblogging services, amidst broader restrictions imposed on social media tools. In December 2011, five major cities (Beijing, Guangzhou, Shanghai, Tianjin, and Shenzhen) announced they would begin requiring microblog services, including the popular Sina Weibo and Tencent, to implement real-name registration. The deadline set for registration was March 16. Those who refused would reportedly have the function enabling them to post messages disabled.[128] In March, Sina announced that it anticipated that about 60 percent of subscribers (over 150 million users) would verify their identity by the deadline, but a counter on the company's website reportedly said only 19 million had registered as of March 16.[129] The counter was then removed and no clear statistics were subsequently available on the scale of the policy's implementation for either Sina or other microblogging services. In April, Sina noted in its annual report to the U.S. Security and Exchange Commission (SEC) that many users had not yet complied, that it feared full implementation would cause its traffic and usage to decline dramatically, and that its ongoing failure to execute full registration exposed it to potentially "severe punishment" by the government.[130] Verification is apparently being done through a government-linked contractor or via users providing their mobile phone number,[131] whose acquisition has required real-name registration since September 2010.[132] This factor led some sources to estimate that by early 2012, approximately 50 percent of microblog users' real identities were indirectly known to providers because they accessed the platform via their already registered mobile phones.[133]

Surveillance of internet and mobile phone communications by security services is pervasive. The same deep-packet inspection technology used to censor content based on banned key words is also used to monitor and detect users trying to access or disseminate similar information. In some free expression cases, private instant-messaging conversations or text messages have been directly cited in court documents. During 2011, two lawsuits were filed in U.S. courts against the American technology company Cisco Systems, asserting there was evidence the firm had customized its surveillance equipment to assist Chinese security agencies in apprehending Falun Gong practitioners and democracy activists; Cisco denied the allegations and the cases were pending as of May 2012.[134] Separately, one academic study reported observing that queries on the search engine Baidu that contained banned keywords were being automatically redirected with the user's IP address to a location in Shanghai suspected of being related to the city's Public Security Bureau.[135] Given the secrecy surrounding such capabilities, however, it is difficult to verify their existence or extent of their use.

Various service providers (including ISPs, bulletin boards, and email providers) are required to retain user information for 60 days and provide it to the authorities upon request without independent judicial oversight.[136] Cybercafes require users to present photo ID and must record user activities. In some regions, video surveillance cameras in cybercafes are reportedly directly connected to the local police station.[137] In recent years, additional intrusive elements have

been added to the surveillance apparatus. In March 2011, Beijing's municipal government announced that it would begin using technology to track the location of the city's 17 million mobile phone users in real time.[138] The declared purpose was to be able to provide up-to-date traffic information to relieve congestion, but the announcement sparked concerns it would be used to identify and punish dissent.[139]

China has emerged as a key global source of cyberattacks. Although not all attacks originating in the country have been explicitly traced back to the government, their scale, organization, and targets have led many experts to believe that they are either sponsored or condoned by Chinese military and intelligence agencies. The assaults have included distributed denial-of-service (DDoS) attacks on domestic and overseas groups that report on human rights abuses, such as Human Rights in China, Aizhixing, Boxun, Falun Gong websites, ChinaAid, and Chinese Human Rights Defenders.[140] In April 2011, the website Change.org, which at the time was carrying a petition calling for the release of Ai Weiwei that had quickly garnered tens of thousands of signatures, was disabled by a sophisticated DDoS attack reportedly originating in China.[141] In June 2011, Google reported that hundreds of Gmail accounts had been targeted by attacks originating in China. Among those targeted were "senior U.S. government officials, Chinese political activists, officials in several Asian countries (predominantly South Korea), military personnel and journalists."[142] Other attacks appeared to have economic motives behind them. In February 2011, U.S. computer security firm McAfee reported that computer networks of at least five multinational oil and gas companies were attacked by a group of hackers based in China for information on oil and gas production systems and financial documents related to these companies' field operation.[143] Extensive cyberespionage networks traced back to China have been detected extending to 103 countries in an effort to spy on the Tibetan government-in-exile and its contacts, including Indian government facilities and foreign embassies.[144] In August 2011, the opposition Democratic Progressive Party in Taiwan charged that hackers from China and Taiwan had accessed their email accounts.[145]

The Chinese government has vigorously denied any involvement in these attacks.[146] Such denials were undermined by archive footage aired on a state-run television program in July 2011, which included a demonstration of software designed by the Chinese military being used to carry out an attack on a Falun Gong-related website in the United States.[147] Similarly, in October 2011, the *Financial Times* reported that many of the 500 employees of Nanhao Group, a technology company based outside Beijing, are part of a militia unit organized by the People's Liberation Army (PLA) to specialize in cyberattacks and cyber defense.[148]

Chinese users have also been victims of cybercrime both from hackers based both inside and outside the country. The government-run National Computer Network Emergency Response Technical Team reported that Chinese computers were targeted in 2010 by about 480,000 Trojan horse viruses, nearly half originating from outside China.[149] In 2012, a military source reported that 8.9 million computers in China were infected with Trojan horse viruses controlled by IP addresses from outside the country. [150]

Notes

1 Lena L. Zhang, "Behind the 'Great Firewall': Decoding China's Internet media policies from the inside," *The International Journal of Research into New Media Technologies*, Volume 12(3), 2006, 271-291.

2 Gary King, Jennifer Pan, and Margaret Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," Working Paper, June 18, 2012, http://gking.harvard.edu/files/censored.pdf.

3 CNNIC, "Information and Updates on the Development of the Internet in China" [Hu Lian Wang Fa Zhan Xin Xi Yu Dong Tai], Issue 72 (Beijing: CNNIC, 2011), http://www.cnnic.cn/research/zx/qwfb/201112/W020111221472293628373.pdf.

4 Zhang Jing, "Internet Monitor System Auto-Filters Reactionary Messages" [Wang Luo Shen Cha Xi Tong Yan Zhi Chen Gong, Fan Dong Xin Xi Zi Dong Guo Lv], Jing Hua Daily, February 26, 2003, http://www.people.com.cn/GB/it/53/142/20030226/931430.html.

5 CNNIC, "The 28th Report on the Development of the Internet in China" [Zhong Guo Hu Lian Wang Fa Zhan Zhuang Kuang Tong], July, 2011, http://www.cnnic.cn/research/bgxz/tjbg/201107/P020110721502208383670.pdf.

6 CNNIC, "Information and Updates on the Development of the Internet in China" [Hu Lian Wang Fa Zhan Xin Xi Yu Dong Tai], Issue 76, May, 2012, http://www.cnnic.cn/research/zx/qwfb/201205/W020120504484883351802.pdf. The International Telecommunications Union (ITU) cited a similar rate of 38 percent in 2011: International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

7 Ibid.

8 International Telecommunication Union, "The World in 2011: ICT Facts and Figures," October, 2011, http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf.

9 CNNIC, "The 29th Report on the Development of the Internet in China" [Zhong Guo Hu Lian Wang Fa Zhan Zhuang Kuang Tong], January, 2012, p.21, http://www.cnnic.cn/dtygg/dtgg/201201/W020120116337628870651.pdf.

10 CNNIC, "The 28th Report on the Development of the Internet in China." [By comparison, in 2010, the percentage was 33.6 from cybercafés.

11 CNNIC, "The 28th Report on the Development of the Internet in China," p.4.

12 James Fallows, "The Connection has been Reset," The Atlantic, March 2008, http://www.theatlantic.com/magazine/archive/2008/03/-ldquo-the-connection-has-been-reset-rdquo/6650/

13 Lu Hui, "China Telecom, China Unicom pledge to mend errors after anti-monopoly probe," English.news.cn, December, 2011, http://news.xinhuanet.com/englisTITLE010/china/2011-12/02/c_131285141.htm.

14 International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

15 CNNIC, "The 28th Report on the Development of the Internet in China," p.4.

16 Chen Jian, "China Internet Polulation Reaches 485 Million, The Number of Microblogging Users Increases Dramatically" [Zhong Guo Wang Min Gui Mo Da 4.85 Yi, Wei Bo Yong Hu Shu Liang Bao Fa Zeng Zhang], Ren Min Wang, July, 2011, http://it.people.com.cn/GB/15192981.html; CNNIC, "Statistical Report on Internet Development in China," January, 2011, p.36, http://www.cnnic.cn/dtygg/dtgg/201201/W020120116337628870651.pdf.

17 Chris Hogg, "China Restores Xinjiang Internet," British Broadcasting Corporation (BBC), May 14, 2010, http://news.bbc.co.uk/2/hi/asia-pacific/8682145.stm.

18 "China police block access to protest village," Telegraph, December 12, 2011, http://www.telegraph.co.uk/news/worldnews/asia/china/8951275/China-police-block-access-to-protest-village.html.

19 Tania Branigan, "China cut off internet in area of Tibetan unrest," Guardian, February 3, 2012, http://www.guardian.co.uk/world/2012/feb/03/china-internet-links-tibetan-unrest.

20 Email communication with Enghebatu Togochog, director of the Southern Mongolia Human Rights Information Center.

21 CNNIC, "Statistical Report on Internet Development in China," accessed March 23, 2009, list of documents: http://www.cnnic.cn/index/0E/00/11/index.htm; Actual document used: http://www.cnnic.cn/uploadfiles/doc/2009/1/13/92209.doc).

22 These include the Public Security, Bureau, State Administration for Industry and Commerce, among others. "A look at an illustration of the whole course of the cybercafe license application process" [Yi Kan Jiu Mingbai Quan Cheng Tu Jie Wang Ba Pai Zhao Shen Qing Liu Cheng], Zol.com, http://detail.zol.com.cn/picture_index_100/index997401.shtml

23 "China Media Bulletin Issue No. 10," Freedom House, February 17, 2011, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-10#state.

24 Zhou Zhi Jun, "Chianed Net Cafes Reached 40%, Government Calling For Establishing Nationwide Net Cafe Association" [Quan Guo Wang Ba Lian Suo Lv 40%, Ni Chou Jian Quan Guo Wang Ba Hang Ye Xie Hui], Ren Min Wang, December 23, 2011, http://game.people.com.cn/GB/48644/48662/16697401.html.

25 "Beijing, Surveillance Software Required Where Wifi Service is Provided" [Beijing: Ka Fei Dian Deng Chang Suo Ti Gong Wu Xian Wang Luo Xu An Zhuang 'Jian Kong Ruan Jian'], Beijing News, July 27, 2011, http://life.gmw.cn/2011-07/27/content_2349463.htm.

26 Zhao Zhuo, "Some Cafe in Beijing Suspened Wifi Service" [Zhao Zhuo, Beijing Bu Fen Ka Fei Ting Ting Zhi Ti Gong Wu Xian Wang Luo], Beijing Youth Daily, http://www.mercicoffee.com/news/china/5565.html.

27 Hung Huang, "Censorship in Chinese Media," Economix, September 25, 2008, http://economix.blogs.nytimes.com/2008/09/25/censorship-in-chinese-media/.

28 For example, a study conducted in 2011 by scholars at Carnegie Mellon found that up to 53 percent of microblog posts generated from Tibet were deleted; http://www.cmu.edu/news/stories/archives/2012/march/march7_censorshipinchina.html

29 These include, for instance, the prodemocracy manifesto Charter 08 and the "Nine Commentaries," a series of editorials analyzing the history of the party and encouraging an end to its rule. See graph, "Inaccessible Sites – Top 100 Google Search Results," from OpenNet Initiative, *Internet Filtering in China in 2004-2005: A Country Study*, available at Select Committee on Foreign Affairs, "Written Evidence Submitted by Sarah Cook, Student at the School of Oriental and African Studies, University of London," House of Commons, Session 2006-07, http://www.publications.parliament.uk/pa/cm200607/cmselect/cmfaff/269/269we08.htm; Nart

Villeneuve, *Breaching Trust: An Analysis of Surveillance and Security Practices on China's TOM-Skype Platform* (Toronto: Information Warfare Monitor/ONI Asia, 2008), http://www.nartv.org/mirror/breachingtrust.pdf; Julen Madariaga, "Charter 08: Why It Should Be Called Wang," Chinayourren, January 11, 2009, http://chinayouren.com/eng/2009/01/charter-08-why-it-should-be-called-wang/.

30 Gary King et al., "How Censorship in China Allows Government Criticism but Silences Collective Expression."

31 Sophie Beach, "Directives from the Ministry of Truth: May 1-31, 2011," June 4, 2011, China Digital Times, http://chinadigitaltimes.net/2011/06/directives-from-the-ministry-of-truth-may-1-31-2011.

32 Gary King et al., "How Censorship in China Allows Government Criticism but Silences Collective Expression."

33 Shley Esarey and Xiao Qiang, "Digital Communication and Political Change in China," *International Journal of Communication*, 5 (2011), 298-319, http://ijoc.org/ojs/index.php/ijoc/article/viewfile/688/525.

34 Ben Wagner, "Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control,'" Global Voices Advocacy, June 25, 2009, http://advocacy.globalvoicesonline.org/2009/06/25/study-deep-packet-inspection-and-internet-censorship/.

35 Joseph Kahn, "China Is Filtering Phone Text Messages to Regulate Criticism," New York Times, July 3, 2004, http://www.nytimes.com/2004/07/03/world/china-is-filtering-phone-text-messages-to-regulate-criticism.html; "Well-red: Chinese communism's classic texts," Economist, February 18, 2010, http://www.economist.com/node/15546357.

36 Xiao Qiang, "A List of Censored Words in Chinese Cyberspace," China Digital Times, August 30, 2004, http://chinadigitaltimes.net/2004/08/the-words-you-never-see-in-chinese-cyberspace/.

37 For example, one academic study reported finding evidence that censorship technology had been placed at the provincial level, enhancing its effectiveness and opening the door to inter-provincial filtering, though there is no evidence to date that is has been used in this manner. See Polverini, Becker, When Form Follows Function: Finding and Modeling Censorware in the People's Republic of China, Princeton University Computer Science Department Thesis Work, 2009, http://www.cs.columbia.edu/bpolveri/papers/bpolverini_pu_thesis.pdf; X. Xu, Z. Mao, and J. Halderman, "Internet Censorship in China: Where Does the Filtering Occur?" *Passive and Active Measurement*, Springer, 2011, 133-142, http://pam2011.gatech.edu/papers/pam2011--Xu.pdf.

38 Tania Branigan, "Internet Censorship in China," The Guardian, January 14, 2010, http://www.guardian.co.uk/world/2010/jan/14/internet-censorship-china; Rebecca MacKinnon, "China Blocks Twitter, Flickr, Bing, Hotmail, Windows Live, etc. Ahead of Tiananmen 20th Anniversary," CircleID, June 2, 2009, http://www.circleid.com/posts/20090602_china_blocks_twitter_flickr_bing_hotmail_windows_live/; Google, "Mainland China Service Availability," accessed July 22, 2010, http://www.google.com/prc/report.html#hl=en; Michael Wines and Andrew Jacobs, "To Shut Off Tiananmen Talk, China Disrupts Sites," New York Times, June 2, 2009, http://www.nytimes.com/2009/06/03/world/asia/03china.html.

39 Keith B. Richburg, "Nervous about unrest, Chinese authorities block Web site, search terms," Washington Post, February 25, 2011, http://www.washingtonpost.com/world/nervous-about-unrest-chinese-authorities-block-web-site-search-terms/2011/02/25/ABPdw5I_story.html.

40 David Barboza and Claire Cain Miller, "Google Accuses Chinese of Blocking Gmail Service," New York Times, March 20, 2011, http://www.nytimes.com/2011/03/21/technology/21google.html.

41 Steven Millward, "Google+ Not Actually Blocked in China, Just Being Slowly Throttled," TechinAsia.com, June 30, 2011, http://www.penn-olson.com/2011/06/30/google-plus-china.

42 Keith B. Richburg and Leila Fadel, "No audience for leaked cables in China and the Arab world," Washington Post, December 2, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/12/01/AR2010120106714.html.

43 Rick Martin, "Ogilvy's 'Social Media Equivalents' in China 2011," TechinAisa.com, October 17, 2011, http://www.penn-olson.com/2011/10/17/china-social-media/.

44 Gary King et al., "How Censorship in China Allows Government Criticism but Silences Collective Expression."

45 Xiao Qiang, "From 'Grass-Mud Horse' to 'Citizen': A New Generation Emerges through China's Social Media Space," Congressional-Executive Commission on China, November 17, 2011, http://www.cecc.gov/pages/hearings/general/hearing1/statement4.pdf.

46 "Self-disciplined Practice and Thoughts of Chinese Internet Industry in Web3.0" [Web3.0 Yuan Nian De Zhong Guo Hu Lian Wang Hang Ye Zi Lv Shi Jian Yu Xi Kao], Wenming.cn, April 2011, http://www.wenming.cn/xwcb_pd/yjpl/201104/t20110407_142975.shtml.

47 "Sina Weibo Over 300 Million Users Now Who generate Over 100MM Posts Everyday," China Internet Watch, February 29, 2012, http://www.chinainternetwatch.com/1395/sina-weibo-users-2011/.

48 Xiao Qiang, "From 'Grass-Mud Horse' to 'Citizen': A New Generation Emerges through China's Social Media Space."

49 Kathrin Hille, "China's Censors Clamp Down On Watchblogger," Financial Times, September 21, 2011, http://www.ft.com/intl/cms/s/0/a5f7a660-e421-11e0-b4e9-00144feabdc0.html#axzz1ZAVEF2y1.

50 "SPECIAL FEATURE, China Media Bulletin No. 29," Freedom House, July 14, 2011, http://freedomhouse.org/sites/default/files/inline_images/Cyberdisappearance%20in%20Action_special_feature-FINAL_0.pdf

51 Xiao Qiang, "From 'Grass-Mud Horse' to 'Citizen': A New Generation Emerges through China's Social Media Space."

52 Zhang Dan, "Alibaba vs Baidu: Can e-commerce trump search?" ZdNet Asia, September 27, 2011, http://www.zdnetasia.com/alibaba-vs-baidu-can-e-commerce-trump-search-62302246.htm.

53 "SPECIAL FEATURE, China Media Bulletin No. 29," Freedom House.

54 "China Media Bulletin: Issue No. 42," Freedom House, December 8, 2011, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-42#To.

55 Ellen Nakashima, Cecilia Kang, and John Pomfret, "Google to Stop Censoring Search Results in China," Washington Post, March 23, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/22/AR2010032202041.html.

56 Loretta Chao, "Chinese Regulators Renew Key License For Google," Wall Street Journal, September 7,2011, http://online.wsj.com/article/SB10001424053111904836104576556203077777200.html

57 Edward Wong and David Barboza, "Wary of Egypt Unrest, China Censors Web," New York Times, January 31, 2011, http://www.nytimes.com/2011/02/01/world/asia/01beijing.html.

58 Sarah Lovenheim, "In China, 'Egypt' and 'Cairo' have vanished," Washington Post, March 2, 2011, http://voices.washingtonpost.com/postpartisan/2011/02/imagine_if_you_typed_egypt.html.

59 Ian Johnson, "Calls for a 'Jasmine Revolution' in China Persist," New York Times, February 23, 2011, http://www.nytimes.com/2011/02/24/world/asia/24china.html; Andrew Jacobs and Jonathan Ansfield, "Catching Scent of Revolution, China Moves to Snip Jasmine," New York Times, May 10, 2011, http://www.nytimes.com/2011/05/11/world/asia/11jasmine.html.

60 For instance, in January 2011, authorities ordered the removal of a satirical animated video that marked the upcoming Year of the Rabbit by mocking a series of scandals that had sparked public anger against the authorities; the clip concluded with an uprising. After initially garnering public attention, it began being systematically deleted from Chinese websites, though it remained available on YouTube, which is blocked. "Little Rabbit Kuang Kuang" [Xiao Tu Zi Kuang Kuang], http://www.youtube.com/watch?v=svwTTCxoJ3A; He Ping, "Animation 'Little Rabbit Kuang Kuang' Deleted from China's Internet" ['Xiao Tu Zi Kuang Kuang' Xi Lie Dong Hua Pian Zao Zhong Guo Hu Lian Wang Shan Chu], Radio Free Asia, January 26, 2011, http://www.rfa.org/mandarin/yataibaodao/tu-01262011164057.html.

61 "China Media Bulletin No. 53," Freedom House, April 12, 2012, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-53#Microblog comments.

62 Ibid.

63 "China Media Bulletin No. 52," Freedom House, March 29, 2012, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-52#Users%20report

64 See, for example, Politburo involvement in planning response to Nobel Peace Prize and Politburo member Liu Changchun's orders to state-run firms to stop doing business with Google: Jacobs, "Tirades Against Nobel Aim at Audience in China"; James Glanz and John Markoff, "Vast Hacking by a China Fearful of the Web," New York Times, December 4, 2010, http://www.nytimes.com/2010/12/05/world/asia/05wikileaks-china.html?pagewanted=1&_r=3.

65 The SIIO operates under the jurisdiction of the State Council Information Office. "China sets up State Internet information office," China Daily, May 4, 2011, http://www.chinadaily.com.cn/china/2011-05/04/content_12440782.htm.

66 "China Media Bulletin No. 21," Freedom House, May 5, 2011, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-21#SIIO.

67 Keith B. Richburg, "China Moves To Rein In Microblogs," Washington Post, October 4, 2011, http://www.washingtonpost.com/world/asia-pacific/china-moves-to-rein-in-microblogs/2011/10/03/gIQAXLLsKL_story.html.

68 Michael Wines and Sharon LaFraniere, "Chinese Protest Suspensions of Bloggers," New York Times, August 26, 2011, http://www.nytimes.com/2011/08/27/world/asia/27weibo.html.

69 Ming De, "Bosses from Leading Telecommunications Companies Attended Authority's Meeting" [Zhong Guo Ge Da Wang Lu Ji Tuan Zong Cai Bei Ban Ban Zuo Bao Zheng], Soundofhope.org, November 6, 2011, http://big5.soundofhope.org/programs/162/202778-1.asp; "China Upgraded Censorship with Cooperation from Telecommunication Industry" [Zhong Guo Kong Zhi Wang Lu Yan Lun Sheng Ji, Ke Ji Ye Zhe Pei He 'Zu Zhi You Hai Zi Xun Chuan Bo'], Taiwan News, November 7, 2011, http://www.taiwannews.com.tw/etn/news_content.php?id=1751337.

70 Michael Wines and Sharon LaFraniere, "Chinese Protest Suspensions of Bloggers," New York Yimes, August 26, 2011, http://www.nytimes.com/2011/08/27/world/asia/27weibo.html.

71 Twitter of Hu Yong, https://twitter.com/#!/huyong/status/38988441538666496; David Bandurski, "Brutality and Tragedy Unseen," China Media Project, February 1, 2012, http://cmp.hku.hk/2012/02/01/18380/; David Bandurski, "Thank Goodness for Hong Kong," China Media Project, January 31, 2012, http://cmp.hku.hk/2012/01/31/18311/.

72 C. Custer, "Ai Weiwei and Politics on Weibo," TechinAisa.com, November 8, 2011, http://www.penn-olson.com/2011/11/08/ai-weiwei-and-politics-on-weibo/; C. Custer, "Sina Blocks Weibo Accounts in Wake of Ai Weiwei's Fundraising Campaign," TechinAisa.com, November 7, 2011, http://www.penn-olson.com/2011/11/07/sina-blocks-weibo-accounts-in-wake-of-ai-weiweis-fundraising-campaign/.

73 "China Media Bulletin No. 47," Freedom House, February 16, 2012, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-47#Party

74 "Sina Weibo Introduces 'User Contract,'" Caijing.com.cn, May 9, 2012, http://english.caijing.com.cn/2012-05-09/111842544.html; "Censorship 3.0? Sina Weibo's New 'User Credit' Points System," China Real Time Report (blog), Wall Street Journal, May 29, 2012, http://blogs.wsj.com/chinarealtime/2012/05/29/censorship-3-0-sina-weibos-new-user-credit-points-system/.

75 Oiwan Lam, "China: The Internet as an Ideology Battlefield," Global Voices Advocacy, January 6, 2010, http://advocacy.globalvoicesonline.org/2010/01/06/china-internet-as-an-ideology-battlefield/.

76 "Interim Provisions on the Administration of Internet Websites Engaged in News Posting Operations," November 1, 2000, excerpts available at http://www.cecc.gov/pages/virtualAcad/exp/explaws.php.

77 Keith B. Richburg, "Chinese Editors, And A Web Site, Detail Censors' Hidden Hand," Washington Post, April 13, 2011, http://www.washingtonpost.com/world/chinese-editors-and-a-web-site-detail-censors-hidden-hand/2011/04/01/AFpMiRSD_story.html; "China Media Bulletin No. 17," Freedom House, April 7, 2011, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-17.

78 David Bandurski, "Ai Weiwei Chat With Opinion Manipulator Surfaces," China Media Project, May 5, 2011, http://cmp.hku.hk/2011/05/09/12125/; Wu Nan, "Chinese Bloggers on the History and Influence of the 'Fifty Cent Party,'" China Digital Times, May 15, 2008, http://chinadigitaltimes.net/2008/05/chinese-bloggers-on-the-history-and-influence-of-the-fifty-cent-party/.

79 David Bandurski, "China's Guerrilla War for the Web," Far Eastern Economic Review, July 2008, http://feer.wsj.com/essays/2008/august/chinas-guerrilla-war-for-the-web; Sarah Cook, "China's Growing Army Of Paid Internet Commentators," Freedom House (blog), October 11, 2011, http://blog.freedomhouse.org/weblog/2011/10/chinas-growing-army-of-paid-internet-commentators.html.

80 David Bandurski, "Internet Spin for Stability Enforcers," China Media Project, May 25, 2010, http://cmp.hku.hk/2010/05/25/6112/.

81 Sarah Cook, "China's Growing Army Of Paid Internet Commentators."

82 Chen Jian, "Sixty Million People Have Participated in 'Red Text Message' Efforts" [Zhong Guo Liu Qian Wan Ren Can Yu Zhuan Fa Shou Ji 'Hong Duan Zi'], Beijing Ren Min Wang, March 16, 2010, http://news.163.com/10/0316/21/61U6BNGM000146BD.html; "China Telecom: Red Text Message – 'Love in China, Opportunities in Guang Dong' Writing Contest" [Hong Duan Zi Zhi 'Ai Wo Zhong Hua Chuang Ye Guang Dong' Wang Luo Chuang Ye Da Sai - - Mei Li Yang Jiang], Baidu, August 21, 2008, http://hi.baidu.com/liming10liming/blog/item/24de0a234ea6cbfad6cae224.html.

83 H. Yu, "Blogging Everyday Life in Chinese Internet Culture," *Asian Studies Review* 31 (2007): 423-33.

84 David Barboza, "Despite Restrictions, Microblogs Catch on in China," New York Times, May 15, 2011, http://www.nytimes.com/2011/05/16/business/global/16blogs.html.

85 Brook Larmer, "Where an Internet Joke Is Not Just a Joke," New York Times, October 26, 2011, http://www.nytimes.com/2011/10/30/magazine/the-dangerous-politics-of-internet-humor-in-china.html.

86 Xiao Qiang, "From 'Grass-Mud Horse' to 'Citizen': A New Generation Emerges through China's Social Media Space."

87 Sharon LaFranierea, "Grass-Roots Fight to Save a 'Supertree,'" New York Times, June 4, 2011, http://www.nytimes.com/2011/06/05/world/asia/05china.html?pagewanted=1.

88 Sharon LaFranierea, "China Finds More Bodies, and a Survivor, in Trains' Wreckage," New York Times, June 25, 2011, http://www.nytimes.com/2011/07/26/world/asia/26wreck.html; Michael Wines and Sharon LaFranierein, "Baring Facts of Train Crash, Blogs Erode China Censorship," New York Times, June 28, 2011, http://www.nytimes.com/2011/07/29/world/asia/29china.html; "China Media Bulletin No. 31," Freedom House, July 28, 2011, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-31.

89 Bloody Map: A map created by Chinese internet users on forced eviction, immolation, and other local government power abuse, at: http://maps.google.com/maps/ms?brcurrent=3,0x35cab73c2e5c4465:0x946f70601c3d2630,0,0x34354978b41cab51:0xf168d14d8f0a2226%3B5,0,0&ie=UTF8&hl=zh-CN&msa=0&msid=111560301092049321699.0004921f02f43f6c4f07e&ll=35.532226,100.283203&spn=55.026174,79.013672&source=embed[2]%20Image:%20http://www.flickr.com/photos/shichuan/5085224907/.

90 J. Lacharite, "Electronic Decentralization in China: A Critical Analysis of Internet filtering Policies in the People's Republic of China," *Australian Journal of Political Science* 37 (2002): 2, 333-46; Guobin Yang, *The Power of the Internet in China: Citizen Activism Online* (New York: Columbia University Press, 2009), http://www.chinese.rfi.fr/%E4%B8%AD%E5%9B%BD/20110216-%E4%B8%AD%E5%AE%A3%E9%83%A8%E8%A6%81%E6%B1%82%E5%AA%92%E4%BD%93%E5%AF%B9%E6%89%93%E6%8B%90%E8%BF%90%E5%8A%A8%E2%80%9C%E9%80%82%E5%BA%A6%E9%99%8D%E6%B8%A9%E2%80%9D.

91 Email communication with circumvention tool developer who wished to remain anonymous, June 2012.

92 Jason Ng, "Investigation of Random Sampling in Chinese Twitter Users" [Zhong Wen Twitter Yong Hu Qun Chou Yang Diao Cha], Kenengba, January 27, 2010, http://www.kenengba.com/post/2540.html.

93 For example, in March 2011, several popular VPNs reported being crippled. In November, administrators of TOR found that many of its "bridge nodes" had become inaccessible to Chinese users shortly after being set up. The managers of other circumvention tools like Ultrasurf and Freegate also witnessed intensified efforts to disrupt their services, though at year's end, Chinese users were still able to access them. Internet security experts confirmed suspicious activity in late 2011, suggesting that Chinese ISPs may have been testing a new system for identifying the type of encrypted services often used by circumvention tools in order to them disconnect them. See, Sharon LaFraniere and David Barboza, "China Tightens Censorship of Electronic Communications," New York Times, March 21, 2011, http://www.nytimes.com/2011/03/22/world/asia/22china.html?_r=2&pagewanted=1; Andy Greenberg, "China's Great Firewall Tests Mysterious Scans On Encrypted Connections," Forbes, November 17, 2011, http://www.forbes.com/sites/andygreenberg/2011/11/17/chinas-great-firewall-tests-mysterious-scans-on-encrypted-connections/.

94 "Written Statement of Li Hai, Falun Gong practitioner and former member of Department of Treat and Law, Ministry of Foreign Affairs, People's Republic of China," Hearing of Foreign Affairs Committee regarding human rights in China, July 25, 2012, http://foreignaffairs.house.gov/112/HHRG-112-FA00-WState-HaiL-20120725.pdf.

95 "The President Order of The People's Republic of China, No.28" [Zhong Hua Ren Min Gong He Guo Zhu Xi Ling, Di Er Shi Ba Hao], http://www.gov.cn/flfg/2010-04/30/content_1596420.htm.

96 Reporters Without Borders, "Amendment Enlists ICT Companies in Protectino of State Secrets," news release, April 29, 2010, http://en.rsf.org/china-amendment-enlists-ict-companies-in-29-04-2010,37238.html; Jonathan Ansfield, "China Passes Tighter Information Law," New York Times, April 29, 2010, http://www.nytimes.com/2010/04/30/world/asia/30leaks.html.

97 Ian Johnson, "Call for Protests in China Draws More Police than Protesters," New York Times, February 27, 2011, http://www.nytimes.com/2011/02/28/world/asia/28china.html; Andrew Jacobs and Jonathan Ansfield, "Well-Oiled Security Apparatus in China Stifles Calls for Change," New York Times, February 28, 2011, http://www.nytimes.com/2011/03/01/world/asia/01china.html.

98 Edward Wong, "Human Rights Advocates Vanish as China Intensifies Crackdown," New York Times, March 11, 2011, http://www.nytimes.com/2011/03/12/world/asia/12china.html.

99 Prepared Statement of Xiaorong Li, Independent Scholar, Congressional-Executive Commission on China Roundtable on "Current Conditions for Human Rights Defenders and Lawyers in China, and Implications for U.S. Policy," June 23, 2011, http://www.cecc.gov/pages/roundtables/2011/20110623/statement4.php.

100 "Tortured, dissident Christian lawyer talks about his ordeal," Asianews.it, September 15, 2011, http://www.asianews.it/news-en/Tortured,-dissident-Christian-lawyer-talks-about-his-ordeal-22641.html; Paul Mooney, "Silence of The Dissidents," South China Morning Post, July 4, 2011, http://pjmooney.com/en/Most_Recent_Articles/Entries/2011/7/4_Silence_of_The_Dissidents.html.

101 Kate Taylor, "Arts Group Calls for Worldwide Sit-In for Ai Weiwei," New York Times, April 14, 2011, http://artsbeat.blogs.nytimes.com/2011/04/14/arts-group-calls-for-worldwide-sit-in-for-ai-weiwei/?scp=9&sq=&st=nyt.

102 "Wu Yu, Ai Weiwei Was Criticized for Pornography, Netizens Fought Back" [Ai Wei Wei Bei Zhi 'Se Qing', Wang Min 'Ai Luo Luo'], Dw.de, November 19, 2011,http://www.dw-world.de/dw/article/0,,15543929,00.html.

103 Sui-Lee Wee, "No interviews, Twitter, travel for Ai Weiwei," Reuters, June 24, 2011, http://www.reuters.com/article/2011/06/24/us-china-artist-idUSTRE75L3U520110624.

104 Prepared Statement of Elisabeth Wickeri, Executive Director and Adjunct Professor of Law, Leitner Center for International Law and Justice, Fordham Law School; Member, Committee to Support Chinese Lawyers, Congressional-Executive Commission on China Roundtable on "Current Conditions for Human Rights Defenders and Lawyers in China, and Implications for U.S. Policy"; Paul Mooney, "Silence of The Dissidents."

105 "China Charges Well-Known Internet Activist with Subversion," Voice of America, March 27, 2011, http://www.voanews.com/english/news/asia/China-Charges-Well-Known-Internet-Activist-with-Subversion-118788199.html; Andy Yee, "China: Ran Yunfei's Blogging for Political Change," Global Voices, April 9, 2011, http://globalvoicesonline.org/2011/04/09/china-ran-yunfei%E2%80%99s-blogging-for-political-change; C. Custer, "Ran Yunfei's Release and Online Activism in China," TechinAsia.com, August 11, 2011, http://www.penn-olson.com/2011/08/11/ran-yunfeis-release-and-online-activism-in-china; Silvia Duarte, "Ran Yunfei Released After Ai Weiwei Asks for Blogger's Support on Twitter," Sampsoniaway.org (blog), August 16, 2011, http://www.sampsoniaway.org/blog/2011/08/16/ran-yunfei-released-after-ai-weiwei-asked-for-bloggers-support-on-twitter.

106 "Document - Futher Information: Chinese Activist Sentenced To Nine Years," Amnesty International, January 6, 2012, https://www.amnesty.org/en/library/asset/ASA17/002/2012/en/888cba41-1a6b-462c-b639-c85f27c6b5ab/asa170022012en.html; "China's 'Jasmine' activists," Amnesty International, May 6, 2011,http://www.amnesty.org.nz/news/china%E2%80%99s-jasmine-activists.

107 "China detains, censors bloggers on 'Jasmine Revolution'," Committee to Protect Journalists, February 25, 2011 http://www.cpj.org/2011/02/china-detains-censors-bloggers-on-jasmine-revoluti.php; Prepared Statement of Xiaorong Li, Independent Scholar, Congressional-Executive Commission on China Roundtable on "Current Conditions for Human Rights Defenders and Lawyers in China, and Implications for U.S. Policy."

108 Charles Hutzler, "Wang Lihong, Chinese Online Activist, Sentenced To Prison For Staging Protest," Huffington Post, September 9, 2011, http://www.huffingtonpost.com/2011/09/09/wang-lihong-prison_n_955226.html; "Internet Activist Wang Lihong Tried in Beijing," China Digital Times, August 16, 2011, http://chinadigitaltimes.net/2011/08/internet-activist-wang-lihong-tried-in-beijing/.

109 "Jailed Human Rights Lawyer Allowed Visit By Brother," Reporters Without Borders, March 29, 2012 http://en.rsf.org/chine-authorities-step-up-pressure-on-30-03-2011,39918.html

110 Cara Anna, "China's Troublemakers Bond Over 'Drinking Tea,'" Associated Press, March 10, 2010, http://abcnews.go.com/Technology/wirestory?id=10062829&page=1; "@StonyWang: Forced to Drink Jasmine Tea," China Digital Times, March 25, 2011, http://chinadigitaltimes.net/2011/03/stonywang-forced-to-drink-jasmine-tea/; "China detains, censors bloggers on 'Jasmine Revolution,'" Committee to Protect Journalists.

111 Andrew Jacobs, "Chinese Government Responds to Call for Protests," New York Times, February 20, 2011, http://www.nytimes.com/2011/02/21/world/asia/21china.html.

112 "China Media Bulletin No. 27," Freedom House, June 30, 2011, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-27#jailed; "China Media Bulletin No. 10," Freedom House, February 17, 2011, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-10#activist.

113 "Liu Xiaobo Briefly Leaves Jail; Wife's House Arrest Continues,"China Digital Times, October 4, 2011, http://chinadigitaltimes.net/2011/10/liu-xiaobo-briefly-leaves-jail-wifes-house-arrest-continues/.

114 Sharon Hom, "Google and Internet Control in China: A Nexus Between Human Rights and Trade?" (testimony, U.S. Congressional-Executive Commission on China, Washington, DC, March 24, 2010), http://www.cecc.gov/pages/hearings/2010/20100324/homTestimony.pdf?PHPSESSID=0e7517d795355cc4cd7132dcb51f2004.

115 Jiang Xun, "New Trend of Chinese Citizens Running for Local People's Congress," The World and China Institute, http://www.world-china.org/newsdetail.asp?newsid=3421

116 "China's New Independents Tap Social Media to Challenge Communist Party (Updated)," China Digital Times, June 8, 2011, http://chinadigitaltimes.net/2011/06/chinas-new-independents-tap-social-media-to-challenge-communist-party/.

117 John Kennedy, "China: Independent Candidates Busy Building Up Support Photos," Global Voices, July 17, 2011, http://globalvoicesonline.org/2011/07/17/china-independent-candidates-busy-building-up-support/.

118 "China's New Independents Tap Social Media to Challenge Communist Party (Updated)," China Digital Times.

119 In July 2012, a Chongqing court ruled in Fang's favor in a lawsuit he filed for administrative compensation over his one year served in the camp. Given the rarity of such victories for labor camp detainees, most observers interpreted the ruling more as a reflection of the change in Bo Xilai's political fortune than as signaling a larger loosening of restrictions on free expression; "China Media Bulletin No.63," Freedom House, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-63#2; "China Media Bulletin No.24," Freedom House, June 9, 2011, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-24#netizen.

120 The pair had uploaded a video online that claimed thousands of police officers were guarding a wedding convoy, suggesting misuse of public resources; local police said the officers were in a training drill and happened to be passing by. Brian Spegele and Josh Chin, "China Detains Pair for Spreading Rumors Online," Wall Street Journal, December 12, 2011, http://blogs.wsj.com/chinarealtime/2011/12/12/china-detains-pair-for-spreading-rumors-online/?mod=google_news_blog; "China detains two for spreading online rumor," China Daily, December 12, 2011, http://www.chinadaily.com.cn/china/2011-12/12/content_14252920.htm.

121 "Six netizens arrested, sixteen websites shut down," IFEX, April 11, 2012, www.ifex.org/china/2012/04/02/netizens_arrested; Wu Ming, "China Human Rights Briefing April 3 -10, 2012," Chinese Human Rights Defenders, April 11, 2012, http://chrdnet.com/2012/04/11/china-human-rights-briefing-april-3-10-2012/.

122 "TCHRD condemns China sentencing of Tibetan Filmmaker Dhondup Wangchen," press release, January 8, 2012, http://www.tchrd.org/report/press/2010.pdf.

123 "Mongolian Professors Held," Radio Free Asia, June 7, 2011, http://www.rfa.org/english/news/china/professors-06072011123731.html/.

124 "Falun Gong News Bulletin: June 10, 2011," Falun Dafa Information Center, June 10, 2011, http://www.faluninfo.net/article/1139/#6.

125 Jonathan Ansfield, "China Web Sites Seeking Users' Names," New York Times, September 5, 2009, http://www.nytimes.com/2009/09/06/world/asia/06chinanet.html; Reporters Without Borders, "Government Crusade Against Online Anonymity," news release, May 7, 2010, http://en.rsf.org/china-government-crusade-against-online-07-05-2010,37412.html.

126 "Ministry of Culture Will Curb Trend of Internet Indecency in 2009" [Wen Hua Bu 2009 Jiang Da Li Zhen Zhi Hu Lian Wang Di Su Zhi Feng], Net Bar China, January 6, 2009, http://www.netbarcn.net/Html/PolicyDynamic/01061954388252.html; Chen Jung Wang, "Real Name System Intimidates High School BBS" [Shi Min Zhi Rang Gao Xiao BBS Bian Lian], CNHubei, November 29, 2009, http://www.cnhubei.com/200511/ca936578.htm; "Internet Society of China: Real Name System for Bloggers is Set" [Zhong Guo Hu Lian Xie Hui: Bo Ke Tui Xing Shi Min Zhi Yi Chen Ding Ju], Xinhua News, October 22, 2006, http://www.itlearner.com/article/3522.

127 Donnie Hao Dong, "Wanna Setup a Personal Website in China? BEING TAKEN a Portrait Please," Blawgdog, February 23, 2010, http://english.blawgdog.com/2010/02/wanna-setup-personal-website-in-china.html; Elinor Mills, "China Seeks Identity of Web Site Operators," CNET News, February 23, 2010, http://news.cnet.com/8301-27080_3-10458420-245.html.

128 "China Media Bulletin No. 46," Freedom House, February 3, 2012, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-46#3.

129 Melanie Lee, "Weibo, China's Twitter, Estimates 60 Percent Of Users Verified By Deadline," Huffington Post, March 12, 2012, http://www.huffingtonpost.com/2012/03/12/weibo-china-twitter_n_1338246.html; Malcom Moore, "China moves to control Sina Weibo social network with real names," The Telegraph, March 16, 2012, http://www.telegraph.co.uk/technology/news/9147767/China-moves-to-control-Sina-Weibo-social-network.html.

130 "China Media Bulletin: Issue No. 46," Freedom House, May 3, 2012, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-56#3.

131 Ibid.; "Real-name Verification of Weibo Suspected Monopolized by Guo Zheng Tong" [Du Zi He Cha Wei Bo Shi Ming Guo Zheng Tong She Long Duan], Hong Kong Commercial Daily, December 30, 2011, http://www.hkcd.com.hk/content/2011-2/30/content_2875001.htm; "Beijing Users of Weibo Required for Real-name Verification of" [Beijing Yao Qiu Wei Bo Yong Shi Ming Fa Yan], BBC, December 16, 2011, http://www.bbc.co.uk/zhongwen/trad/chinese_news/2011/12/111216_beijing_weibo.shtml.

132 "Mobile phone real name system implemented today, SIM card purchasers have to present their ID documents" [Shou Ji Shi Ming Zhi Jin Qi Shi Shi, Gou Ka Xu Chi Shen Fen Zheng], News 163, October 1, 2010, http://news.163.com/10/0901/00/6FF3HKF8000146BD.html.

133 Net.China.com.cn, March 15, 2012 [in Chinese], http://net.china.com.cn/txt/2012-03/15/content_4875947.htm.

134 Somini Sengupta, "Group Says It Has New Evidence of Cisco's Misdeeds In China," New York Times, September 2, 2011, http://www.nytimes.com/2011/09/03/technology/group-says-it-has-new-evidence-of-ciscos-misdeeds-in-china.html; "Suit claims Cisco helped China repress religious group," Thomson Reuters News & Insight, May 20, 2011, http://newsandinsight.thomsonreuters.com/Legal/News/2011/05_-_May/Suit_claims_Cisco_helped_China_repress_religious_group/; Don Tennant, "Second Lawsuit Accuses Cisco of Enabling China to Oppress Citizens, " IT Business Edge, June 9, 2011, http://www.itbusinessedge.com/cm/blogs/tennant/second-lawsuit-accuses-cisco-of-enabling-china-to-oppress-citizens/?cs=47334; Mark Chandler, "Cisco Supports Freedom of Expression, an Open Internet and Human Rights," The Platform, Cisco Blog, June 6, 2011, http://blogs.cisco.com/news/cisco-supports-freedom-of-expression-an-open-internet-and-human-rights/.

135 Becker Polverin and William M. Pottenger, "Using Clustering to Detect Chinese Censorware," Eleventh Annual Workshop on Cyber Security and Information Intelligence Research, Article No. 30, 2011, http://www.cs.columbia.edu/bpolveri/papers/Polverini-abstract-4pgs.pdf.

136 "China," OpenNet Initiative, August 9, 2012, http://opennet.net/research/profiles/china-including-hong-kong.

137 Ibid.; Naomi Klein, "China's All-Seeing Eye," NaomiKlein.org, May 14, 2008, http://www.naomiklein.org/articles/2008/05/chinas-all-seeing-eye.

138 "Beijing plans to track mobile phone users in real-time" [in Chinese], Yahoo News, March 3, 2009, http://news.cn.yahoo.com/ypen/20110303/237829.html.

139 Cecilia Kang, "China Plans to Track Cellphone Users, Sparking Human Rights Concerns," Washington Post, March 3, 2011, http://voices.washingtonpost.com/posttech/2011/03/china_said_it_may_begin.html.

140 Maggie Shiels, "Security Experts Say Google Cyber-Attack Was Routine," BBC, January 14, 2010, http://news.bbc.co.uk/2/hi/technology/8458150.stm; "ChinaAid Websites Collapse Under Repeated Malicious Cyber Attacks," Persecution.org, December 2, 2010, http://www.persecution.org/2010/12/02/chinaaid-websites-collapse-under-repeated-malicious-cyber-attacks/ .

141 Benjamin Joffe-Walt, "Chinese Hackers Attack Change.org Platform in Reaction to Ai Weiwei Campaign," Change.org (blog), April 19, 2011, http://blog.change.org/2011/04/chinese-hackers-attack-change-org-platform-in-reaction-to-ai-weiwei-campaign/.

142 "Ensuring your information is safe online," Google Official Blog, June 2, 2011, http://googleblog.blogspot.com/2011/06/ensuring-your-information-is-safe.html.

143 "John Markoff, Hackers Breach Tech Systems of Oil Companies," New York Times, February 10, 2011 http://www.nytimes.com/2011/02/10/business/global/10hack.html.

144 Information Warfare Monitor and Shadowserver Foundation, "Shadows in the Cloud: Investigating Cyber Espionage 2.0," April 6, 2010, http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0; 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.

145 Chris Wang, "Hackers Attack DPP's Presidential Campaign Office," Taipei Times, August 10, 2011, http://www.taipeitimes.com/News/front/archives/2011/08/10/2003510374/1

146 Michael Wines, "China Rejects Google's Hacking Charge," New York Times, June 6, 2011, http://www.nytimes.com/2011/06/07/world/asia/07china.html; Reuters, "China state newspaper disputes cyber-hacking involvement," Guardian, August 5, 2011, http://www.guardian.co.uk/technology/2011/aug/05/china-cyber-hacking-denied-mcafee; Michael Riley, "Morgan Stanley Attacked By China-Based Hackers Who Hit Google," Bloomberg, March 1, 2011, http://www.bloomberg.com/news/2011-02-28/morgan-stanley-network-hacked-in-same-china-based-attacks-that-hit-google.html.

147 Edward Wong, "China State TV Deletes Video Implying Hacking of Western Sites," New York Times, August 26, 2011, http://www.nytimes.com/2011/08/27/world/asia/27china.html; Ellen Nakashima and William Wan, "China's Denials About Cyberattacks Undermined By Video Clip," Washington Post, August 25, 2011, http://www.washingtonpost.com/world/national-security/state-media-video-candidly-depicts-chinas-developing-cyber-weaponry/2011/08/22/gIQAqyWkbJ_story.html; Ellen Nakashima and Jason Ukman, "Chinese cyberwar video goes missing," Washington Post, August 25, 2011, http://www.washingtonpost.com/blogs/checkpoint-washington/post/chinese-vanish-cyberwar-video

-that-caused-stir/2011/08/25/gIQAAK8edJ_blog.html; CCTV subsequently deleted the clip, but it is still viewable on YouTube: http://www.youtube.com/watch?v=L_Wu1HlZbBk&feature=youtu.be&t=36s.

148 "China Tech Companies Have Army-Linked 'Cybermilitias,'" China Media News, October 13, 2011, http://www.chinamedia.com/2011/10/13/china-tech-companies-have-army-linked-cybermilitias/.

149 Michael Kan, "China Hit by 480,000 Trojan Horse Attacks in 2010," PCWorld, August 10, 2011, https://www.pcworld.com/businesscenter/article/237662/china_hit_by_480000_trojan_horse_attacks_in_2010.html.

150 Jia Lei and Cui Meng, "Ma Xiaotian Appeals for Suppressing 'Cyber Armament Race'" [Ma Xiao Tian Yu E 'Wnag Luo Jun Bei Jing Sai'], Takungpao, May 29, 2012, http://www.takungpao.com.hk/news/12/05/29/ZM-1484251.htm.